Encentuate® Identity and Access Management (IAM)

Administrator Guide

Product version 3.6

Document version 3.6.5

Copyright notice

Encentuate® IAM Administrator Guide version 3.6.5

NO WARRANTY: Any documentation made available to you is as is, and Encentuate makes not warranty of its accuracy or use. Any use of the documentation or the information contained herein is at the risk of the user.

Documentation may include technical or other inaccuracies or typographical errors. Encentuate reserves the right to make changes without prior notice.

Trademarks

Contact information

For more information about this product or any support enquiries, contact us:

To log a support incident: https://customercare.encentuate.com

To reach us by phone:

- Americas: +1-800-ENCENTUATE ext 5 (+1-866-362-3688 ext 5)
- Asia Pacific: +65-6862-7085

Email: customercare@encentuate.com

Table of Contents

Troubleshooting 151

Appendices

About This Guide

Welcome to the Encentuate IAM Administrator Guide.

Use this guide to configure and manage the different components of Encentuate IAM Enterprise.

Purpose

This guide provides procedures to help install, administer and test Encentuate IAM Enterprise. It aims to cover the functionality and setup options of the product including internal implementation details (such as, describes what the product does and how to set it up).

Audience

The target users for this deployment guide are highly technical users that can understand how an Encentuate product can be enhanced and customized for a specific customer's use.

What's in this guide

IAM Overview provides an introduction to the Encentuate Identity and Access Management Suite's features.

Installing The IMS Server contains the minimum requirements and instructions for successfully installing the IMS Server. It also discusses how to integrate IMS with an enterprise's directory services.

Configuring The IMS Server contains a procedure on how to use the Setup Assistant feature of AccessAdmin.

Installing AccessAgent covers various options of installing AccessAgent.

Maintaining The IMS Server illustrates the Encentuate IMS Server Architecture, and several ways of using and maintaining the IMS Server.

Searching and Managing Users discusses how to manage users with Encentuate AccessAdmin.

Setting Policies covers general procedures for setting user and system policies.

Managing Policy Templates defines policy templates, and discusses how to view, modify, create and delete templates for users and machines.

Searching and Managing Machines discusses how to manage machines with Encentuate AccessAdmin.

Reports and Audit Logs covers how to view system properties using Encentuate AccessAdmin; how to view and print audit reports; how to audit logs; and how to maintain audited logs.

Configuration Tips provides useful information when configuring Encentuate IMS Server.

Troubleshooting discusses how to deal with the different problems you may encounter while using and configuring Encentuate IMS Server.

Installing The IMS Database covers the pre-requisites in installing the IMS database.

Definitions of policies details policy attributes, description, and provides instructions on how to set policies to achieve different results.

Using The IMS Configuration Utility contains reference information on how to manipulate the IMS Configuration Utility to control the behavior of Encentuate IMS Server.

Document conventions

Refer to this section to understand the distinctions of formatted content in this guide.

Main interface elements

The following are highlighted in bold text in the guide: dialog boxes, tabs, panels, fields, check boxes, radio buttons, fields, buttons, folder names, policy IDs/names, and keys. Examples are: **OK**, **Options** tab, and **Account Name** field.

Navigation

All content that helps users navigate around an interface is italicized (for example: *Start >> Run >> All Programs*)

Cross-references

Cross-references refer you to other topics in the guide that may provide additional information or reference. Cross-references are highlighted in green and display the referring topic's name (for example: Document conventions).

Hyperlinks

Hyperlinks refer you to external documents or web pages that may provide additional information or reference. Hyperlinks are highlighted in blue and display the actual location of the external document or web page (for example: http://www.encentuate.com).

Scripts, commands, and code

Scripts, commands, or codes are those entered within the system itself for configuration or setup purposes, and are usually formatted in Courier font.

For example:

```
<script language="JavaScript">

<!--

  ht_basename = "index.php";

  ht_dirbase = "";

  ht_dirpath = "/" + ht_dirbase;

//-->

</script>
```

Tips or Hints

Tips or hints help explain useful information that would help perform certain tasks better.

Warnings

Warnings highlight critical information that would affect the main functionalities of the system or any data-related issues.

IAM Overview

With an increasing number of enterprise applications with multiple access points, organizations now face the challenge of providing convenient access and ensuring strong security. The rise in criminal hacking activity and the looming threat of cyber-terrorism makes this challenge even greater.

Many security compromises occur due to weak passwords. A study shows that one-third of end user passwords can be broken in less than five minutes. To counter such threats, enterprises must strengthen access control systems. Passwords are not only the weakest link in the security chain, they are also very expensive to support.

A large number of passwords create a security challenge and a management problem. It is estimated that an enterprise spends an average of US$150-$400 per user per year on password management. To reduce password management costs, enterprises may consider conventional single sign-on solutions.

While conventional single sign-on reduces password management costs, it also increases an organization's vulnerability by replacing multiple application passwords with a single password to the single sign-on server, thereby creating a key to the kingdom problem.

Multiple weak application passwords and conventional single sign-on are not the right solutions for the enterprise. These solutions simplify access, but weaken security. What enterprises need are enterprise access security solutions. Solutions that simplify, strengthen, and track access for all digital and physical assets.

This section covers the following topics:

- About the Encentuate IAM Suite
- Components of Encentuate IAM
- Authentication factors
- Usage configuration
- Encentuate icons
- Policies, certificates, and other product concepts

About the Encentuate IAM Suite

The Encentuate® Identity and Access Management (IAM) Suite empowers enterprises to automate access to corporate information, strengthen security, and enforce compliance at the enterprise end-points. With Encentuate IAM, enterprises can efficiently manage business risks, achieve regulatory compliance, decrease IT costs, and increase user efficiency. With Encentuate, enterprises do not have to choose between strong security and convenience.

The Encentuate IAM Suite delivers the following capabilities – without requiring changes to the existing IT infrastructure.

Strong authentication for all user groups

Encentuate IAM provides strong authentication for all user groups – inside and outside the corporate perimeter – to prevent unauthorized access to confidential corporate information and IT networks. The solution leverages multi-factor authentication devices, such as USB smart card tokens, building access badges, proximity cards, mobile devices, photo badges, biometrics, and one-time password (OTP) tokens.

In addition to comprehensive support for authentication devices, Encentuate IAM focuses on leveraging existing identification devices and technologies for authentication. Encentuate IAM also provides iTag, a patent-pending technology that can convert any photo badge or personal object into a proximity device, which can be used for strong authentication.

Enterprise single sign-on with workflow automation

With Encentuate Single Sign-On (ESSO), users can enjoy fast access to all corporate applications (e.g., web, desktop, TTY and legacy) and network resources with the use of a single, strong password on personal and shared workstations.

This feature helps enterprises increase employee productivity, lower IT Helpdesk costs, and improve security levels by eliminating passwords and the effort of managing complex password policies.

Encentuate IAM improves speed to access information by up to 85% via SSO and workflow automation on shared and personal workstations. Users can automate the entire access workflow (e.g., application login, drive mapping, application launch, single sign-on, navigation to preferred screens, multi-step logins, etc.).

Single Sign-Off and configurable desktop protection policies ensure protection of confidential corporate applications from unauthorized access. If a user walks away from a workstation without logging out, Encentuate IAM can be configured to enforce inactivity timeout policies (e.g., configurable screen locks, application logout policies, graceful logoff, etc.).

Comprehensive session management capability

As organizations deploying more shared workstations and kiosks, more users can roam and access information from anywhere without having to return to their personal PCs. Shared and roaming scenarios pose severe security threats.

When users walk away without logging off from workstations or share generic logins, they risk exposing confidential information to unauthorized access. Any attempt to tighten security, enforce unique user logins, and comply with regulations leads to users being locked out of workstations, which results in efficiency losses.

With Encentuate IAM, organizations can increase user convenience and improve information security through session management or fast user switching capabilities, depending on the access needs user groups. Users can quickly sign-on and sign-off to shared workstations without using the Windows domain login process, picking up their work where they left off.

Additionally, fast user switching on private desktops allows users to maintain multiple unique user desktops on the same workstation, preserving each user's applications, documents, and network drive mappings.

If a user walks away from a session without logging out, Encentuate IAM can be configured to enforce inactivity timeout policies. Encentuate IAM also supports hybrid desktops where organizations combine different session management capabilities to meet the needs of their user community.

User-centric access tracking for audit and compliance reporting

With Encentuate IAM's Audit & Compliance functionality, organizations can consolidate data, manage user-centric, secure, and tamper-evident audit capabilities across all end-points (e.g, personal or shared workstations, Citrix, Windows Terminal Services, or browsers).

When combined with Encentuate's strong authentication capabilities, the user-centric audit logs ensure secure access to confidential corporate information and accountability at all times. The logs provide the meta-information that can guide compliance and IT Administrators to a more detailed analysis – by user, by application, or by end-point.

In addition, this information is collated in a central relational database facilitating real-time monitoring and separate reporting with third party reporting tools.

Organizations can also leverage the end-point automation framework to audit custom access events for any application – without modifying the application or leveraging the native audit functionalities.

Secure remote access anywhere and anytime

Encentuate Secure Remote Access provides browser-based single sign-on to all applications (e.g., legacy, desktop, and Web) from outside the firewall. Organizations can effectively and quickly enable secure remote access for their mobile workforce without installing any desktop software and modifying application servers.

Remote workers require one password, and an optional second authentication factor to access information from remote offices, home PCs, and PDAs. Once access is granted, users can sign-on to applications by clicking on the application links in the Encentuate portal. Access can be protected through SSL VPN.

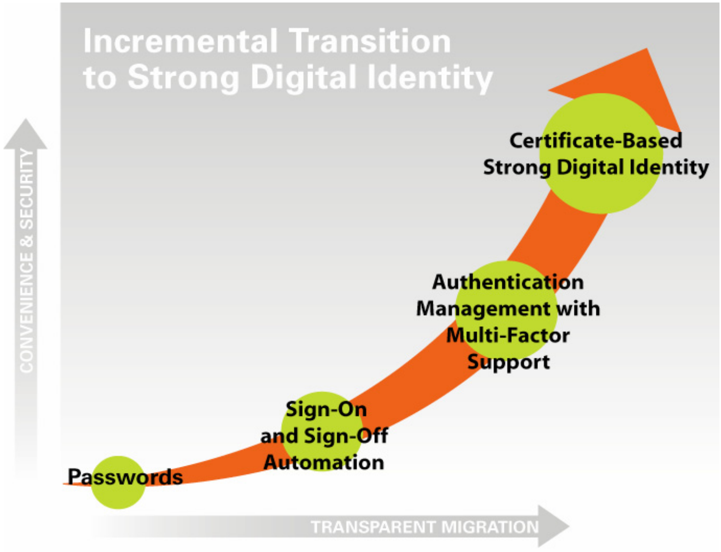
Integration with user provisioning technologies

Encentuate IAM combines with best-of-breed user provisioning technologies to provide end-to-end identity lifecycle management. New employees, partners, or contractors get fast and easy access to corporate information upon being provisioned. Once provisioned, users can leverage single sign-on to access all their applications on shared and personal workstations with one password.

Users are never required to register their user names and passwords individually as their credentials are automatically provisioned.

Building a strong digital identity

Encentuate IAM combines sign-on and sign-off automation, authentication management, and user tracking to provide a seamless path to strong digital identity.



- **No change in user behavior**
- **Incremental, low-risk transition without any user involvement**
- **Future proof architecture**

Encentuate IAM accelerates the adoption of strong digital identity by transparently increasing security, enhancing user convenience, and providing integrated access across existing information, network and physical systems.

Encentuate IAM incrementally transitions enterprise access from password authentication to strong digital identity-based authentication in the following manner:

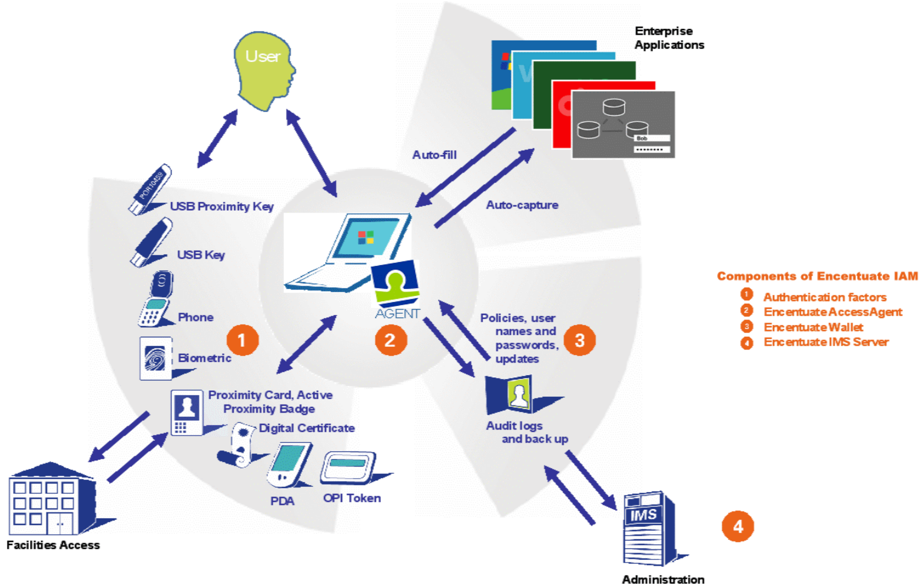
Step 1: Provide sign-on and sign-off automation to enterprise applications

Step 2: Fortify sign-on with authentication management

Step 3: Provide seamless transition from passwords to certificates

Illustrated workflow

The following diagram provides an overview of the core components of the Encentuate IAM solution. The following sections provide an overview of the key components.



Encentuate IAM workflow

The main components of Encentuate IAM are:

- Encentuate Wallet
- Encentuate AccessAgent
- Encentuate AccessAdmin
- Encentuate AccessAssistant

- Encentuate AccessStudio
- Encentuate IMS Server
- Encentuate Web Workplace

To use Encentuate AccessAgent, you must set:

- Encentuate password
- Secret

Based on your organization's security policy, you may be required to use either of the following second authentication factors:

- Encentuate ActiveCode
- Encentuate USB Key
- Encentuate USB Proximity Key
- Encentuate RFID Card
- Encentuate Active Proximity Badge
- Encentuate Fingerprint Identification

Components of Encentuate IAM

The following sections provide an overview of the key components of Encentuate IAM.

Encentuate Wallet

The Encentuate Wallet stores the user's access credentials and related information (including user IDs, passwords, certificates, encryption keys). Each user has a Wallet, with a lock that protects each Wallet. The lock can be as simple as an Encentuate password, or can be fortified with a second authentication factor. The use of the Wallet is governed by a set of security policies.

The Wallet can be located at any point of access where an Encentuate AccessAgent is installed.

Cached Wallet

A "cached" Wallet is a copy of the user's Wallet which is stored in the hard disk of the computer. The user can retrieve the cached Wallet during emergencies (for example, access without IMS Server connectivity.)

In an environment where computers are regularly shared by several users, a user may have access to several computers. In this scenario, caching a Wallet saves a lot of time for the user, and does not require regular downloaded of Wallet from the IMS server again for each use. The Wallet can also be cached in the computer.

Encentuate AccessAgent

Encentuate AccessAgent is the client software that manages the user's Wallet, enabling automatic sign-on to applications and strong authentication. It manages user names, passwords, and digital certificates between the Encentuate Wallet and the IMS Server.

However, the Encentuate AccessAgent does not store passwords. Passwords are stored in the Encentuate Wallet, and therefore known only by the rightful user. Users can also use it to conveniently manage credentials.

The different functions of Encentuate AccessAgent are as follows:

- Password management

  The Encentuate Wallet of AccessAgent remembers and enters user names and passwords for different applications.

- Consolidation of user credentials

  In the background, the Encentuate Wallet of AccessAgent remembers user names for different applications used by an user and sends them to the IMS Server for consolidation.

- Backing up of user credentials

  AccessAgent synchronizes user credentials on the IMS Server to ensure that if users lose their authentication factors or forget their passwords, their user credentials can be recovered.

- Enforcement of password policies

  Enterprise password policies that automatically change passwords to keep them dynamic are specified in IMS Server and enforced by AccessAgent.

- Logging of user and system actions

  Actions performed by users or actions related to Wallet or AccessAgent are logged in log files, synchronized with the IMS Server and consolidated.

Encentuate USB Key Utility

An add-on module to AccessAgent that provides an Administrator with functions to reset Encentuate USB Keys.

Encentuate AccessAdmin

Encentuate AccessAdmin is the management console used by Administrators and Helpdesk officers to manage users and policies on an IMS Server.

Different access rights are given to the Administrator and Helpdesk roles. Certain configurations (for example, system policies) can only be viewed but not modified by Helpdesk. Like the AccessAgent UI, AccessAdmin has a left navigation panel for accessing various functions, such as:

- User search and administration (to modify user policies, issue authorization code, unlock a locked Wallet, revoke user, etc.)
- Creating and maintaining policy templates (can only be created and maintained by an Administrator, but a Helpdesk officer can view and apply)
- Setting system and application policies (can only be modified by an Administrator, but a Helpdesk officer can view)
- Accessing logs and status information

Encentuate AccessAssistant

Encentuate AccessAssistant is the web-based interface used to provide password self-help. Users use AccessAssistant to obtain the latest credentials to log on to their applications.

Using AccessAssistant, users can access their application passwords from a Web browser without AccessAgent installed on the computer. This feature can be enabled or disabled for the user. Mobile ActiveCode or a Helpdesk-issued authorization code can be used as a second authentication factor for authentication to AccessAssistant. Secret questions and answers can also be used to bypass the authorization code requirement, so that users will not have to call Helpdesk.

Encentuate AccessStudio

Encentuate AccessStudio is the wizard based tool used by the Administrator to create and manage AccessProfiles and enable SSO, sign-off, and workflow automation. Each application is represented by an AccessProfile, which is a set of instructions that defines the workflow for that particular application.

Encentuate IMS Server

The Encentuate IMS Server is an integrated management system that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, and authentication policies. It also provides loss management of authentication tokens, certificate management and audit management for the enterprise.

The IMS Server interfaces with other applications through IMS Connectors and IMS Bridges. It is the IMS Server that interfaces with other identity management systems. The IMS Server uses a special IMS Connector, called a messaging connector, to send MACs to users. See Encentuate ActiveCode for a description of Mobile ActiveCode (MAC).

The IMS Server can be configured via AccessAdmin, which is a Web interface for Administrators and Helpdesk to search for and provision users, set policies, and view audit logs and reports. Lower-level configuration settings for the IMS Server can be configured via the IMS Configuration Utility, which is accessible by Administrators.

Encentuate IMS Server is responsible for identity management, certificate management, and recording administrative, user and system actions in audit logs.

A backup of the user's Wallet's contents is stored on the IMS Server, so AccessAgent can retrieve the backed-up information by connecting to the IMS Server with a proper authentication. The information is encrypted and cannot be read by anyone, including Helpdesk officers and Administrators.

IMS Server is an application server that is used for.

- Managing Encentuate Wallet and authentication factors

  Helpdesk officers and Administrators can view the type of Encentuate authentication factor the user is using. Using AccessAdmin, a Wallet can be revoked denying the user access to the Wallet and passwords. It can also be used a reference point to see all the identities the user has in the enterprise. The Administrator can then go into each application and turn off the user's access.

- Managing policies

  Encentuate IAM uses policies to control the behavior of its components. These policies are configurable through various means, so Encentuate IAM can meet the requirements of specific organizational requirements. Policies have different visibility and scope, and are managed by different roles.

  Policies may be applicable system-wide, or only to certain groups of users. The applicability of a policy is determined by its scope, which can be System, User, or Machine.

- System: Policy is system-wide
- User: Policy affects only a specific user
- Machine: Policy affects only a specific machine

All policies can be configured via AccessAdmin. Changes to these policies are propagated to clients the next time AccessAgent synchronizes with the IMS Server.

Administrators can also choose to apply policies to a group of users, by using the search function to find a specific group of users, then applying a set of policies to the select group.

- Managing certificates

  The IMS Server has a a built-in Certificate Authority that manages certificates. See Credentials for more information about certificate management.

- Maintaining logs

  Actions performed by users, Helpdesk officers, Administrators are all logged in log files providing a comprehensive audit trail.

  The IMS Server produces detailed logs of its activities and is also responsible for collating AccessAgent's logs. This provides the Administrator a centralized view of the enterprise's operations. All logs are stored in the database. Encentuate IMS Server logs can be viewed using a custom report generator like Crystal Reports or customers can create their own reports.

IMS service modules

Add-on modules that extend the basic services (user management, policy management, and certificate issuance, etc.) provided by the IMS Server.

IMS bridge

An IMS service module that enables applications to use the Encentuate IMS Server as an authentication server.

IMS connector

An IMS Service Module that enables the IMS Server to interface with other applications as a client, extending the capability of the IMS Server.

Encentuate Web Workplace

A Web-based interface that gives users the ability to log on to enterprise Web applications by clicking on links, without the need to remember the passwords for individual applications. It can be integrated with the existing portal or SSL VPN.

Authentication factors

Encentuate authentication factors come in different forms and functions. With the exception of password and fingerprint, users access systems and applications with a device that works like a key. This concept makes it easy for users to adopt to the system quickly. USB Keys, for example, are about the same size as a car or home key, making it non-intrusive. An RFID Card is about the size of a credit card, and can be easily attached to a key ring.

Encentuate password

The Encentuate password is used to secure access to an Encentuate Wallet. The user specifies this password upon signing up with Encentuate AccessAgent. Signing up with Encentuate AccessAgent means registering the user with the IMS Server, and creating an Encentuate Wallet.

Secret

The user is asked to enter a secret when signing up for an Encentuate Wallet. A secret is a second password or a backup password. It is similar to the “hint” provided when the user forgets the password for a Web e-mail account, for example. The secret should be something that:

- the user will not forget, even if it is not used for a long time
- is not likely to change

When the user signs up, the user selects a Question from a list, and then provides the Answer to that question. If the Encentuate password is forgotten, the secret will help the user to set a new Encentuate password. The user can also use the secret, along with an authorization code, to gain temporary access to the Wallet. An authorization code is generated by a Helpdesk officer or an Administrator.

If self-service is enabled, users may have to specify a number of secrets during sign up. They can provide a subset of these secrets to perform password resets without using an authorization code.

Second authentication factors

The Encentuate password can be fortified by a second authentication factor. The combination of the password and a USB Key, for example, strengthens the user’s computer’s security because both authentication factors must be present to access the computer.

Based on your organization’s security policy, you may be required to use one of the following authentication factors.

Encentuate ActiveCode

The Encentuate ActiveCodes are short-term authentication codes that are controlled by the Encentuate IAM system.

There are two types of ActiveCodes:

- Mobile ActiveCode

  An Encentuate Mobile ActiveCode is a one-time password that is randomly generated and event-based. The Mobile ActiveCode is generated on the IMS Server and delivered via a secure second channel, such as text services (SMS) on mobile phones. It is used for strong authentication.

- Unified ActiveCode

  The Encentuate Unified ActiveCode is a predictive one-time password used for strong authentication. The Unified ActiveCode generator is built into AccessAgent. Software-only Clients will be available for: Windows, PocketPC, PalmOS, and Macintosh. A Unified ActiveCode can also be generated onboard by the Encentuate USB Key.

The use of ActiveCodes enhances the security of traditional password-based authentication for applications, because ActiveCodes are random passwords that can only be used once by an authorized user. Combined with alternative channels and devices, ActiveCodes provide effective second-factor authentication.

Encentuate USB Key

The Encentuate USB Key is a removable USB drive that combines the utility and storage capacity of Flash RAM, the security of a smart card, and the universal connectivity of Universal Serial Bus (USB) into one package. Encentuate's USB Key can store user names, passwords, certificates, encryption keys, and other security credentials.

The USB form factor is cost-effective. No additional hardware is required for the Key to work now that USB ports are available on various platforms. The USB Key stores more passwords and certificates than any other authentication device in the market. The size of the memory can vary according to the needs of your organization. Depending on company policy, users may be allowed to store passwords for personal applications and websites.

✓ *This version also supports Charismathics USB Keys.*

Internally, the USB Key stores the following:

- Serial Number

  The serial number is a unique number embedded in the USB Key during manufacturing. It is also printed on the casing of the USB Key. The number is unique for each USB Key and cannot be changed.

- Common Symmetric Key

  The Common Symmetric Key (CSK) is used to encrypt information that is communicated to the Encentuate IMS Server for backup. Each user has a different and unique CSK.

- Digital certificates for each certificate-enabled application

- Driver for the USB Key, and installation files for Encentuate AccessAgent

  Your computer cannot communicate with a device until a special program is installed. The program is known as a *driver*. The USB Key may require a driver for it to work with your computer. The required drivers can be found in the USB Key, and are detected and installed automatically.

  The files required for installing AccessAgent on your computer are also available in the Encentuate USB Key.

Encentuate USB Key/USB Proximity Key

Encentuate USB Proximity Key

The Encentuate USB Key can be equipped with RFID (Radio Frequency Identification), an electronic device that uses radio frequency signals to read identification information stored within. The USB Key with RFID integration is called the Encentuate USB Proximity Key.

The USB Proximity Key requires a proximity reader to work. The proximity reader is installed on your computer for use with Encentuate AccessAgent, or on any other hardware that requires authorization to use. For example, your office front door or elevator can have a proximity reader so that access is restricted to those with an RFID built into their Encentuate USB Key.

Encentuate RFID Card

The Encentuate RFID Card is an electronic device that uses radio frequency signals to read identification information stored within. RFID (Radio Frequency Identification) works on the concept of proximity; the user needs to tap the RFID Card on the RFID reader to gain access to credentials.

The RFID reader is an additional hardware that needs to be installed on every machine where the RFID Card is used for authentication.

Unlike the USB Proximity Key, the RFID Card does not have any storage capacity.

Encentuate RFID Card also allows for unified access. It can be used to access your computer, as well as for physical security (to access doors, elevators, etc.).

Encentuate RFID Card and reader

Encentuate Active Proximity Badge

The Encentuate Active Proximity Badge works in an almost identical way as the regular RFID Card - it has RFID, and works with a proximity reader. However, the Active Proximity Badge slightly differs in the range that it covers. With the regular Encentuate RFID Card, the card needs to be in very close proximity with the reader.

Encentuate Active Proximity Badge and reader

With the Active Proximity Badge, the distance can be specified. For example, your Active Proximity Badge can be two metres away from the reader, yet it will be recognized.

The reader automatically detects the user's action. For example, when the user leaves the workstation, AccessAgent locks the screen, or logs the user off - depending on the default setting.

Encentuate Fingerprint Identification

The Encentuate Fingerprint Identification system recognizes your fingerprint as an authentication factor. The fingerprint reader translates your fingerprint into encrypted codes, which in turn logs you on to AccessAgent on your computer.

Fingerprint reader

Presence detectors

A presence detector is a device that detects the presence of the user in its vicinity. If affixed to a computer, it can notify AccessAgent when someone comes in front of the computer or goes away. This eliminates the need to manually lock the computer when you need leave it for a short period of time.

Sonar device

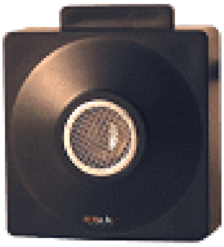
The sonar-based presence detector is used to lock a workstation immediately when the user walks away without waiting for the desktop inactivity time-out. The device uses 40 kHz ultrasonic sound waves (frequency too high for people to hear). It can detect from a range of 5 inches to 5 feet. The user can move within the zone without triggering a walk-away event.

The device is attached to a computer via the USB port and is configured by the system as a keyboard. When the user walks away from the computer, the device sends keystrokes to the computer. Likewise, when the user approaches the computer, the device can be configured to send a different set of keystrokes to the computer. AccessAgent can be configured to intercept these keystrokes and perform appropriate actions (for example, lock the computer.)

The sonar device should not be used with Active Proximity Badge since Active Proximity Badge is itself a presence detector.

Any other supported authentication factors can be used with the pcProx-Sonar:

- Password only
- RFID
- Fingerprint
- USB Key



Sonar device

The behavior can be configured to be very similar to Active Proximity Badge. except that it cannot be used to identify the user as it does not have any ID. The sonar can be combined with building badges (RFID cards) to create a full-proof solution.

Active Proximity Badge

Active Proximity Badge is both a 2nd factor as well as a presence detector as it is able to detect the presence of the user and AccessAgent can be configured to perform appropriate actions.

See Policies for the recommended policy settings for using Active Proximity Badge as a presence detector.

✓ *The presence detector policies (for example, pid_presence_detector_enabled) are not applicable to Active Proximity Badge.*

Usage configuration

Encentuate IAM supports two main usage configurations – personal workstation and shared workstation. For recommended policy settings based on usage configuration, refer to Policies.

Personal workstation configuration

The personal workstation configuration is more applicable for organizations where users are assigned individual workstations. The USB Key is the recommended authentication factor for this type of usage configuration. The setup procedure and workflow are the same regardless of the selected authentication factor.

The user signs up from EnGINA, desktop, or a locked computer at start-up and inserts the USB Key. There is also an option to sign up without the USB Key and register later when it is already available. Signing up without the USB Key, allows the user to log on to AccessAgent subsequently with just an Encentuate password provided it is set in the authentication policy.

To lock computer, remove the USB Key. To unlock the computer, re-insert the USB Key.

Shared workstation configuration

The shared workstation configuration is for organizations where users share common workstations. This usage configuration requires efficient switching between users.

Authentication factors (except the USB Key) are recommended for this type of usage configuration.

IAM supports fast user switching through the following schemes.

- Fast user switching through shared desktop
- Fast user switching through private desktop
- Fast user switching through roaming desktop

These schemes do not use the Windows XP Fast User Switching feature.

To determine which scheme to deploy, consider the following:

- Customer requirements
- Customer budget
- Limitations of each scheme
- Applications that must be supported
- Authentication factors to be used
- Workstations' memory and speed

Fast user switching through shared desktop

Shared Desktops allow multiple users to use one generic Windows desktop in a workstation without having to log on to Windows. Thus, switching of users can be very fast.

When switching from User A to User B, the applications of User A are lost. When the workstation switches back to User A, the applications must be relaunched. This scheme requires AccessProfiles to be created to automatically log off enterprise applications when user switching occurs.

RFID is the authentication factor used in the described Shared Workstation with Shared Desktop configurations.

Users sign up (from EnGINA, desktop, or a locked computer) and tap their RFID cards. Users can also sign up without their RFID cards and register later when the cards are already available. After completing the sign-up process, the user is then logged on to AccessAgent.

When a different user taps the RFID card, switching is invoked, either from the desktop or from the locked computer screen.

After the new user supplies a valid Encentuate password, AccessAgent will unlock the computer (if locked), log off the previous user, and then log on to the new user's Wallet. The new user may not need to supply an Encentuate password if the user is already logged on to other computers with the same RFID+Password in a set time range during the day.

Fast user switching through private desktop

Private Desktops allow multiple users to have their own Windows desktops in a workstation. When a previous user returns to the workstation and unlocks it, AccessAgent switches to the user's desktop session and resumes the last task. However, an existing desktop may have to be logged off if the workstation runs out of resources (for example, memory) for accepting a new user logon. However, if the user logs on to another workstation, the user must relaunch the application.

This scheme uses the Local User Session Management feature of AccessAgent, that uses an IAM component called Encentuate Desktop Manager to manage multiple desktops on a single workstation.

Since logging on from the EnGINA welcome screen is not supported by Local User Session Management, workstations are configured to automatically log on to a generic Windows account upon start-up, and then the computer is locked.

This generic Windows account must not be a registered Encentuate user. It is recommended that a local machine account be used.

All users log on to the workstation from the locked screen. Users tap their RFID cards during sign-up. They also can sign up without the RFID cards and register these later when already available. After completing the sign-up process, the user is logged on to AccessAgent.

AccessAgent is not logged on if you are using an auto-admin account.

When another user taps the RFID card to switch desktop, this user logs on (if without an existing invisible session) or unlocks the workstation (if with an existing invisible session).

The following Wallet authentication options are currently supported:

- Password
- RFID+Password
- Active Proximity Badge+Password
- Fingerprint

If users log on to Windows sessions using their own Active Directory credentials, Local User Session Management requires that synchronization of Encentuate password and Active Directory password be enabled.

However, in some deployments, not all users may have Active Directory accounts. In this case, Local User Session Management can be configured to make use of a pool of computer accounts (either Local machine or Active Directory account) to create the user desktop, and synchronization of Encentuate password and Active Directory password would not be required.

Fast user switching through roaming desktop

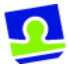
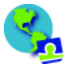
Roaming Desktops allow users' Windows desktops to "roam" to the users' points of access, from workstation to workstation. With roaming sessions, the user can disconnect desktop or application session at one client, log on to another client, and continue desktop or application session at the new client. This scheme requires the use of Terminal Server or Citrix, and hence, is more costly to deploy.

This setup is especially useful for a shared workstation environment, where users roam from one workstation to another, depending on the user's current location.

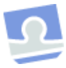
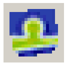
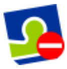
Encentuate icons

Refer to the commonly used icons in Encentuate IAM.

Application icons

Icon	Description
	This icon represents Encentuate AccessAgent application on the desktop.
	This icon represents Encentuate IMS Server on the desktop.

Notification area icons

Icon	Description
	No user has logged on to AccessAgent.
	AccessAgent is operating normally. When the icon is flashing, AccessAgent is: ■ writing data to the USB Key's smart card ■ synchronizing a USB Key with the IMS Server ■ logging the user on
	Auto sign-on is currently disabled.

Policies, certificates, and other product concepts

Credentials

Credentials refer to user names, passwords, certificates, and any other information required for authentication. An authentication factor can serve as a credential. In Encentuate IAM, credentials are stored and secured in the Wallet.

Enterprise identity

In an enterprise, users have multiple user accounts for different applications—e-mail, portal, HR system, web access, and the like. One of these identities is used to authenticate users, and provide access to the enterprise network. For example, users may be required to log on to Windows by entering their user name and password to access the network. This is also known as *enterprise identity*.

The solution that an enterprise uses for identity management must be identified. The solution helps to verify the identities of users logging on with Encentuate Keys. It also links the IMS Server with the directory that the enterprise uses to manage their users.

This policy is set before deployment and sets the foundations of how the system will work. It can be changed later using AccessAdmin, but this action is not recommended. The enterprise identity binding must be a system or application that the enterprise sees as a long term investment and will not be changed, removed or replaced in the near future.

Enterprise applications

The enterprise must select the applications to be included in the enterprise application list.

Enterprise applications are specific to the business of an enterprise and controlled by an Administrator. Some characteristics of an enterprise application:

- Managed through the IMS Server by the information technology department of the enterprise
- Passwords are grouped by authenticating directories
- Audit logs are generated and stored in the IMS Server
- User accounts are pre-created
- User account entry cannot be deleted in AccessAgent
- Passwords can be fortified
- Password entry cannot be set to Never in AccessAgent

Some examples of enterprise applications are: Microsoft Windows, Lotus Notes, Active Directory, SAP, PeopleSoft, Oracle, and Novell.

Enterprise applications can be added, or removed after deployment. However, this is implemented as a global policy, which means all users have access to the same enterprise applications.

Personal applications

The enterprise needs to specify if they will allow users to use AccessAgent and Encentuate Keys for personal applications. Personal applications are applications for which users can specify if they want AccessAgent to store and enter their user name and password. Some examples of personal applications are Yahoo! Mail, Hotmail, ICQ, online banking sites, and the like.

This policy is implemented as a global policy, where users will either be allowed or not allowed to use AccessAgent with personal applications. You cannot grant or deny access to specific users.

User, system, and machine policies

Encentuate IAM uses policies to control the behavior of its components. These policies are configurable through various means, so Encentuate IAM can meet the requirements of specific organizational requirements. Policies have different visibility and scope, and are managed by different roles.

Policies may be applicable system-wide, or only to certain groups of users. The applicability of a policy is determined by its scope, which can be System, User, or Machine.

- System: Policy is system-wide
- User: Policy affects only a specific user
- Machine: Policy affects only a specific machine

System, machine, and user policies can be configured via AccessAdmin. Changes to these policies are propagated to clients the next time AccessAgent synchronizes with the IMS Server (e.g., usually in 20 minutes).

IMS applies machine policies to machines once they join the IMS Server, which are then automatically synchronized with AccessAgent. There can be several machine policy templates defined in IMS. One of these templates is set as default.

Through AccessAdmin, system policies and machine policies can be modified by an Administrator. However, a Helpdesk officer can only view system and machine policies. User policies, however, can be modified by both an Administrator and a Helpdesk officer.

A policy may be defined for different scopes. For example, the desktop inactivity policy may define the desktop inactivity time out duration for one machine or for the entire system. If this policy is defined for both scopes, a priority is defined, in case the time out value is different for the machine and for the entire system.

If the policy priority is “machine”, only the machine policy would be effective. A Command Line Tool (CLT) allows Administrators to view and set policy priorities. For more information, see Setting policy priorities.

Policies may be dependent on other policies. For example, Encentuate hot key action policy is only effective if the Encentuate hot key is enabled. If the latter is disabled, whatever setting for Encentuate hot key action policy will not have any effect on users.

Some groups of policies have overlapping scopes. For example, all these policies have system scope, but the range of entities that they affect are different:

- Wallet inject password entry option default policy. This policy defines the default password entry option for all authentication services and applications.

- Authentication inject password entry option default policy. This policy defines the default password entry option for a specific authentication service.

- Application inject password entry option default policy, which defines the default password entry option for a specific application.

In general, application-specific policies override authentication service-specific policies, which in turn, override general Wallet policies. Therefore, in this case, the Wallet inject password entry option default policy is used when the other two policies are not defined for a particular authentication service or application.

However, if the Authentication service inject password entry option default policy is defined for an authentication service, it will override Wallet inject password entry option default policy when a default password entry option is needed for the authentication service. Similarly, if Application inject password entry option default policy is defined for a particular application, it will override the other two policies.

In a similar way, user-specific policies override system-wide policies. Hence, if a policy has both user and system scopes, for example, the Authentication accounts maximum policy, the user scope setting is always effective if it is defined. If the user scope setting is not defined for a particular user, the system scope setting will become effective.

Certificates in Encentuate IAM

There are four types of certificates in Encentuate IAM:

- Device Property Certificate

  The Device Property Certificate (DPC) is stored in a USB Key and is used to identify the Key's and Hardware Security Module's (HSM) properties. Information in the certificate may include serial number, manufacturing date, manufacturer, and form factor.

- IMS Client Certificate

  The IMS Client Certificate is stored in a USB Key and is used by AccessAgent for authentication when connecting to the IMS Server.

- IMS Server Certificate

  The IMS Server Certificate is stored in the IMS Server and is used to identify an IMS Server.

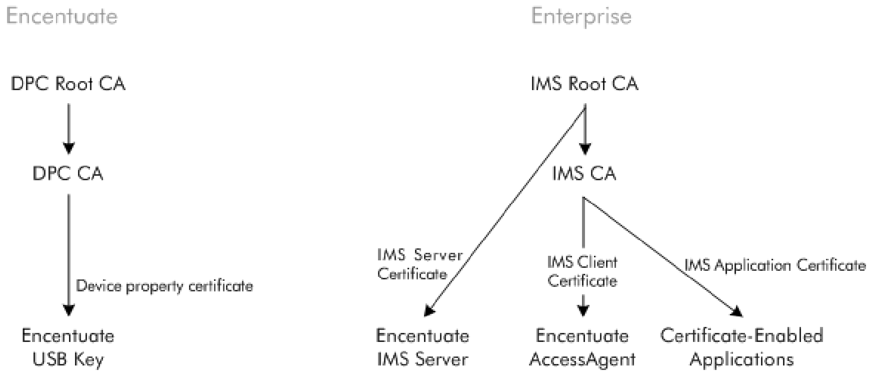
- IMS Application Certificate

  The IMS Application Certificate is stored in a USB Key and is used by a certificate-enabled application to authenticate a USB Key.

Trusted entities

In Encentuate IAM, there are two trusted entities. The first is the Device Property Certificate (DPC) Root CA which resides at Encentuate, and the second is IMS Root CA which is located at the enterprise. Under the DPC Root CA you will find the DPC CA which is responsible for issuing the DPC to a USB Key.

The IMS Root CA has a subordinate certificate authority called IMS CA. IMS CA issues IMS Client Certificate, and IMS Application Certificate to AccessAgent, IMS Server and certificate-enabled applications respectively.

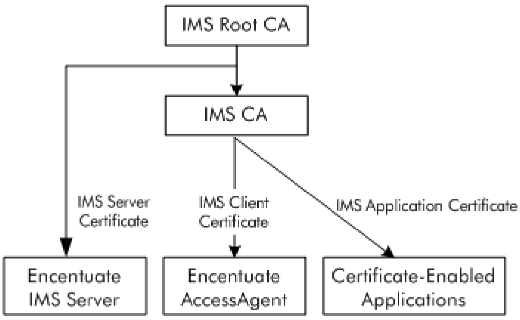


AccessAgent trusts IMS Root CA to communicate with the IMS Server via SSL. It also trusts DPC Root CA to store DPCs in its trust store.

Encentuate Server trusts IMS CA so it can accept IMS Client Certificates. It also trusts DPC Root CA so it can accept DPC during registration.

IMS Root CA management

On top of the hierarchy is IMS Root CA. Below it is the IMS CA, a subordinate CA certified by IMS Root CA to issue certificates. The IMS CA issues IMS Server, Client and Application certificates.

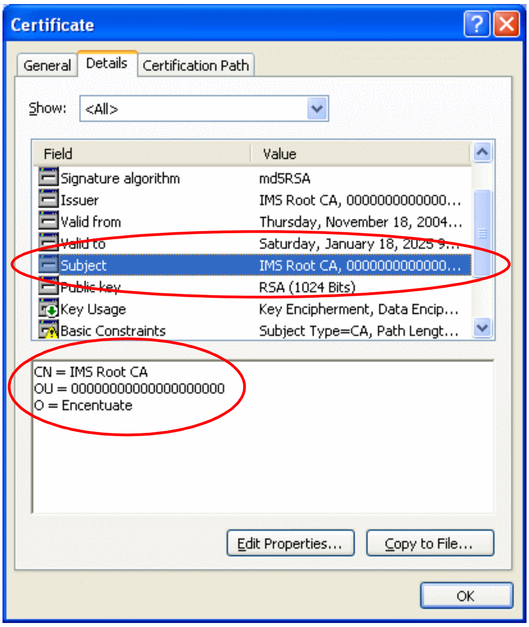


Upon deployment of Encentuate IAM, the enterprise has one IMS Root CA and is responsible for managing it. The IMS Server is programmed to implicitly trust the IMS Root CA.

An IMS Root CA resides in a USB Key. The private key of the IMS Root CA is generated within the Key using RSA. Tamper-proof features of the USB Key ensure that the private key never leaves the Key. The USB Key is also protected by a password allowing for two-factor authentication, securing the private key further.

IMS Root CA signs its own certificate since there is no higher certifying authority then the Root CA in the hierarchy.

If you were to view a certificate issued by IMS Root CA, the *subject* field would look something like this: `CN, OU, O` where `CN` is the name given to the IMS Root CA, `OU` is the serial number of the Key and `O` is the name of the enterprise.



Field	Value
Signature algorithm	md5RSA
Issuer	IMS Root CA, 0000000000000...
Valid from	Thursday, November 18, 2004...
Valid to	Saturday, January 18, 2025 9:...
Subject	IMS Root CA, 0000000000000...
Public key	RSA (1024 Bits)
Key Usage	Key Encipherment, Data Encip...
Basic Constraints	Subject Type=CA, Path Lengt...

CN = IMS Root CA
OU = 00000000000000000000
O = Encentuate

Subject field

IMS Root CA certificates are issued for a period of 20 years because they are trusted by many entities and do not provide digital signatures frequently.

The following security guidelines are recommended for handling a USB Key that contains the IMS Root CA:

- The enterprise should appoint a senior executive to act as the security officer.
- The officer will be given the USB Key and will be responsible for keeping it safe.

The USB Key that contains the IMS Root CA is only used to install IMS Server and renew certificates.

Installing The IMS Server

This section discusses how to set up Encentuate IMS Server. Follow the instructions, depending on the type of installation you will be doing—new or an upgrade.

- Installation prerequisites
- Installing the IMS Server
- Upgrading an existing installation of IMS Server
- Integrating with an enterprise's directory services
- Using the Setup Assistant (IMS Configuration Utility)

Installation prerequisites

Before you install IMS Server, ensure that you meet the following requirements:

- Windows XP, Windows 2000 Server, or Windows 2003 Server
- The monitor's resolution should be at least 256 colors
- Ports 80 and 443 are available

  If any of the ports are being used, disable the applications that are using them. For example, Windows XP automatically starts Internet Information Server (IIS) on port 80. If you use Windows XP, you must disable IIS to make port 80 available.
- Encentuate IMS Server and Encentuate AccessAgent installation CDs.

Express installation

- If Microsoft SQL Server Express Edition/MSDE is already installed on this computer, you must have an Administrator (SA) account and password for Microsoft SQL Server instance.
- If Microsoft SQL Server Express Edition/MSDE is not already installed on this computer, you must have:

- Microsoft Data Access Components (MDAC) 2.8 SP1 or above
- Microsoft Windows Installer 3.1
- Microsoft .NET Framework 2.0
- Microsoft Windows 2000 SP4
- Microsoft Windows XP SP2
- Microsoft Windows 2003 SP1

Custom installation

- For Microsoft SQL Server 2000:
  - Microsoft SQL Server 2000 (Standard, Enterprise or Desktop Edition) with Service Pack 3 and SQL Server Authentication enabled
  - Administrator (SA) account and password for Microsoft SQL Server
- For Microsoft SQL Server 2005:
  - Microsoft SQL Server 2005 (Standard, Enterprise or Express Edition) with Service Pack 1 and SQL Server Authentication enabled
  - Administrator (SA) account and password for Microsoft SQL Server
- For Oracle:
  - Oracle 9i/10g Database with an instance created for the Encentuate IMS Server
  - Administrator (DBA) account and password for this instance, to be used by the Encentuate IMS Server
- For installing database server locally:
  - Microsoft Data Access Components (MDAC) 2.8 SP1 or above
  - Microsoft Windows Installer 3.1
  - Microsoft .NET Framework 2.0

Refer to Installing The IMS Database for more information.

Before installing the IMS Server, make sure your database and the SQL Server Agent have been started and that the SQL authentication is enabled.

Installing the IMS Server

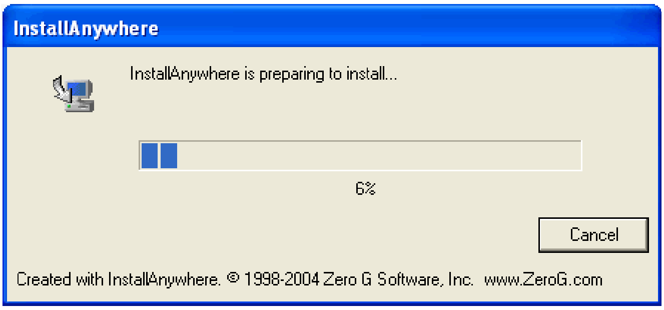
To install the IMS Server:

❶ Insert the Encentuate installation CD.

❷ Go to *Start >> Run...*, click **Browse...**, and click **My Computer**. Right-click on the CD drive and select **Explore**.

❸ Click on **imsinstall.exe** icon in the Encentuate installation CD.

❹ InstallAnywhere extracts the installation files.



InstallAnywhere

InstallAnywhere is preparing to install...

6%

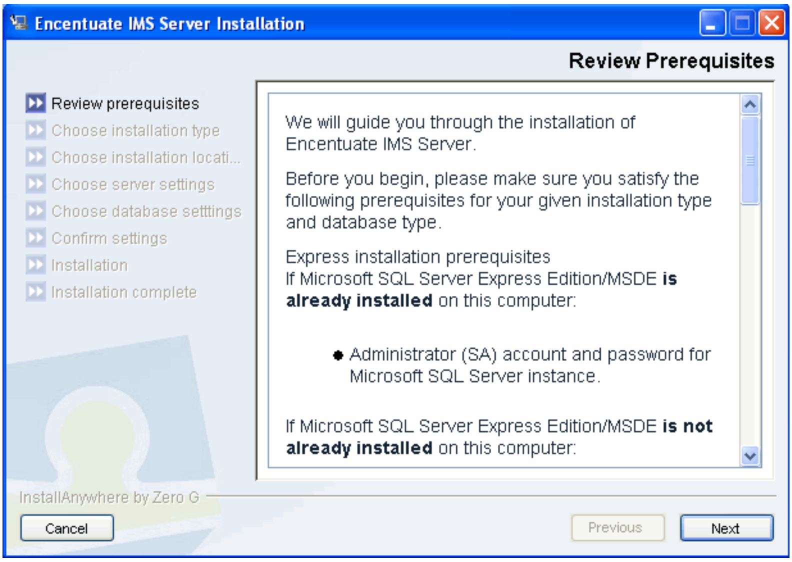
Created with InstallAnywhere. © 1998-2004 Zero G Software, Inc. www.ZeroG.com

Extraction of installation files

❺ The initial screen tells you to make sure you have the required setups, otherwise the installation will not proceed. Ensure you meet all the requirements before you continue.

For more information on the requirements, see Installation prerequisites.

Click **Next**.



We will guide you through the installation of Encentuate IMS Server.

Before you begin, please make sure you satisfy the following prerequisites for your given installation type and database type.

Express installation prerequisites
If Microsoft SQL Server Express Edition/MSDE **is already installed** on this computer:

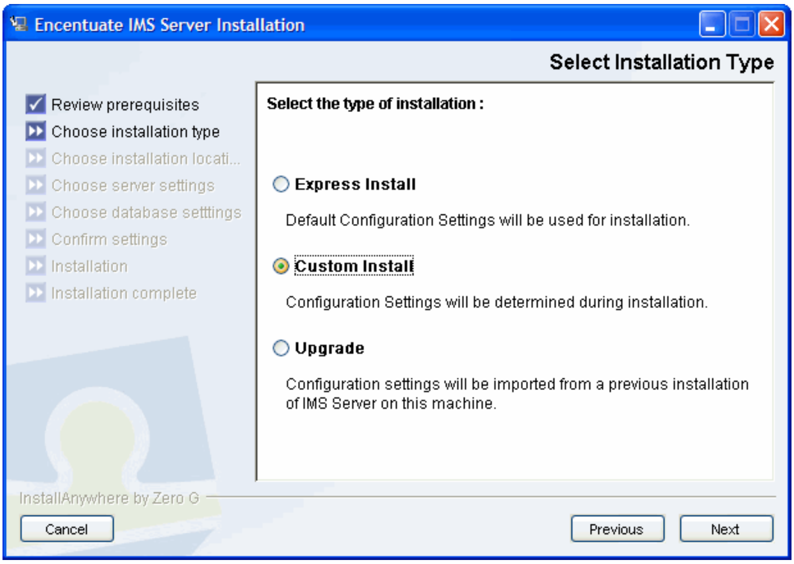
- Administrator (SA) account and password for Microsoft SQL Server instance.

If Microsoft SQL Server Express Edition/MSDE **is not already installed** on this computer:

Review prerequisites

6. Select the installation type. Mark the **Custom Install** option. Click **Next**.

For this procedure, custom installation will be described.



Select the type of installation :

○ **Express Install**

Default Configuration Settings will be used for installation.

● **Custom Install**

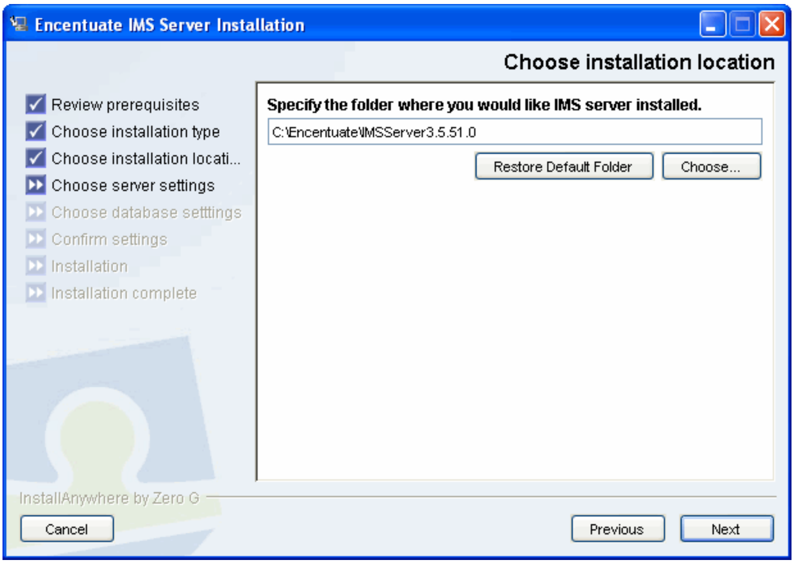
Configuration Settings will be determined during installation.

○ **Upgrade**

Configuration settings will be imported from a previous installation of IMS Server on this machine.

Select installation type

7. Select the installation path where all the installation files will be stored. A recommended path containing the name and version of the IMS Server appears in the field.


Encentuate IMS Server Installation
Choose installation location
☑ Review prerequisites
☑ Choose installation type
☑ Choose installation locati...
Choose server settings
Choose database setttings
Confirm settings
Installation
Installation complete
InstallAnywhere by Zero G
Cancel
Previous
Next

Specify the folder where you would like IMS server installed.

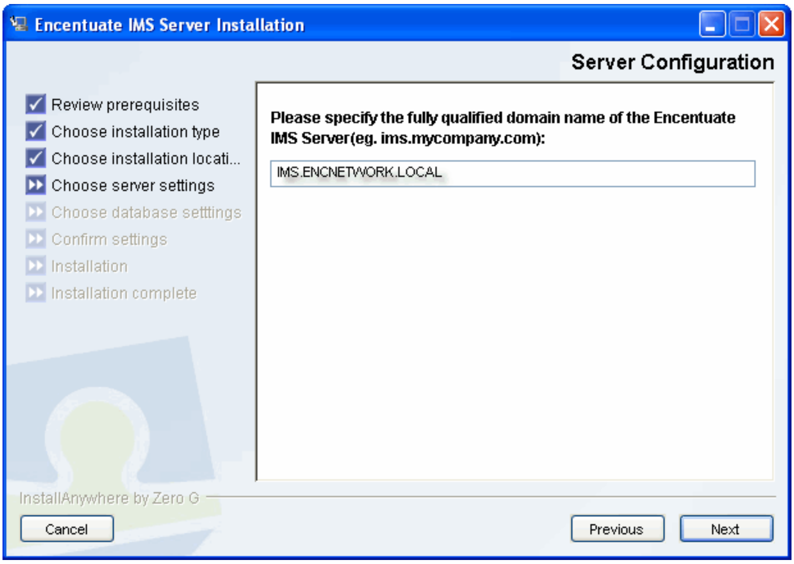
C:\Encentuate\IMSServer3.5.51.0

Restore Default Folder | Choose...

Select installation path

Click **Choose...** to customize the path and browse through your local hard drive. If you modify the path and revert to original recommended path later, click **Restore Default Folder**. Click **Next**.

8. Specify the hostname of the computer on which you are installing the Encentuate IMS Server. The hostname must be resolvable by all users. This is the same hostname that users must specify when they are installing AccessAgent and signing up a Wallet. Click **Next**.

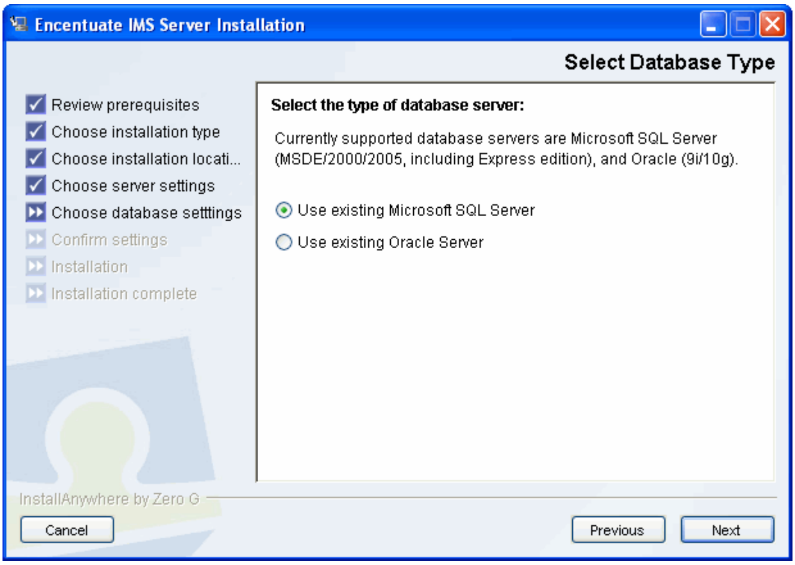

Encentuate IMS Server Installation
Server Configuration
☑ Review prerequisites
☑ Choose installation type
☑ Choose installation locati...
Choose server settings
Choose database setttings
Confirm settings
Installation
Installation complete
InstallAnywhere by Zero G
Cancel
Previous
Next

Please specify the fully qualified domain name of the Encentuate IMS Server(eg. ims.mycompany.com):

IMS.ENCNETWORK.LOCAL

Specify IMS server hostname

9. Select the type of database to use for the system. Click **Next**.



Encentuate IMS Server Installation

Select Database Type

Select the type of database server:

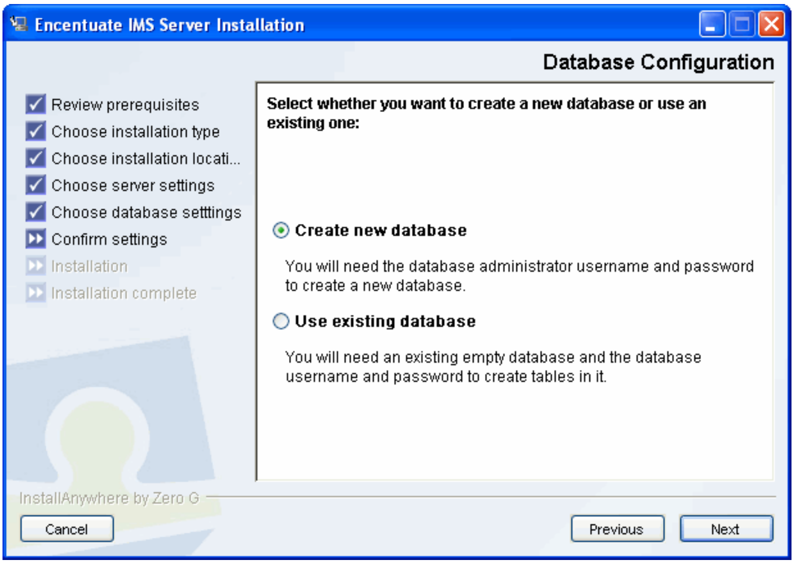
Currently supported database servers are Microsoft SQL Server (MSDE/2000/2005, including Express edition), and Oracle (9i/10g).

● Use existing Microsoft SQL Server

○ Use existing Oracle Server

Select database type

⓾ Specify whether you will create a new database or use an existing one.



Encentuate IMS Server Installation

Database Configuration

Select whether you want to create a new database or use an existing one:

● **Create new database**

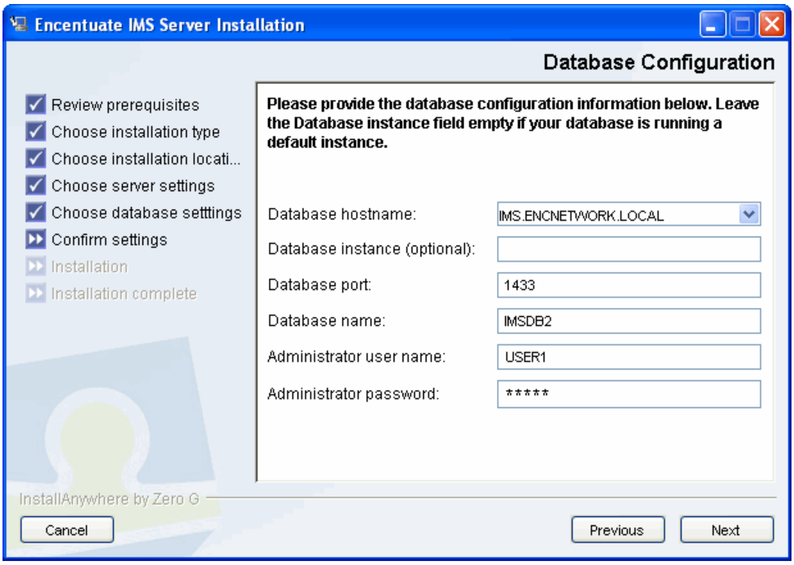
You will need the database administrator username and password to create a new database.

○ **Use existing database**

You will need an existing empty database and the database username and password to create tables in it.

Database configuration

⓫ In Database Configuration, specify the database host, port, and name. Enter your Administrator user name and password. Provide the name of the server where the database is located.



Encentuate IMS Server Installation

Database Configuration

Please provide the database configuration information below. Leave the Database instance field empty if your database is running a default instance.

Database hostname: IMS.ENCNETWORK.LOCAL

Database instance (optional):

Database port: 1433

Database name: IMSDB2

Administrator user name: USER1

Administrator password: *****

Database configuration

For MS SQL Server, the **Database Instance Name** may be left blank (indicating default). However, if you are using an Oracle database, you must specify the instance name.

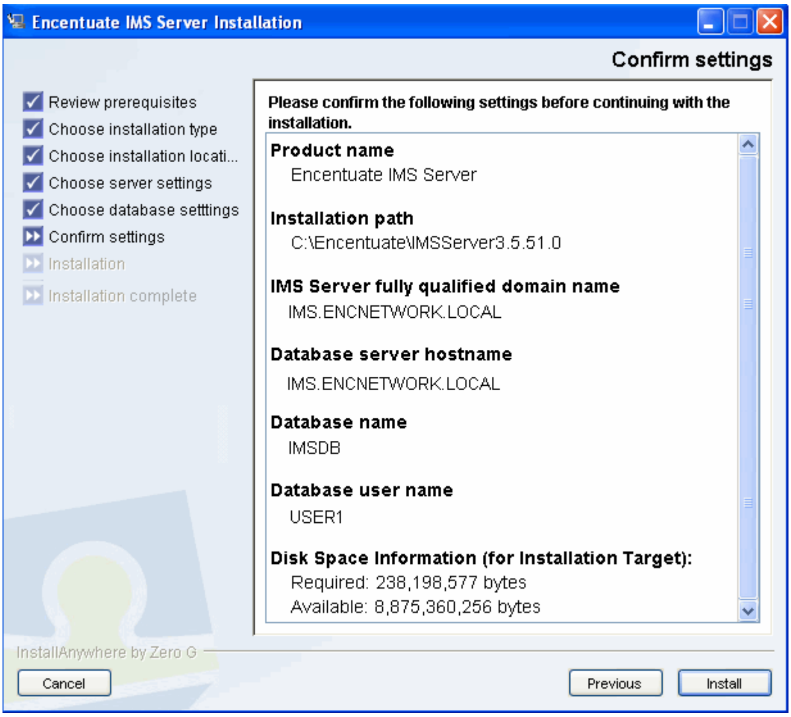
Enter the user name and password that will be used to connect to the database server.

Click **Next**.

The username and password entered must NOT be the database Administrator (Sa) account.

The installer checks if the database is ready. When connection settings are verified, the installation continues.

⑫ The Pre-Installation Summary window shows the details of your preferred configuration. Verify if all the settings are correct. To make changes before installing, click the **Previous** button.


Encentuate IMS Server Installation
Confirm settings
☑ Review prerequisites
☑ Choose installation type
☑ Choose installation locati...
☑ Choose server settings
☑ Choose database setttings
Confirm settings
Installation
Installation complete
InstallAnywhere by Zero G
Cancel
Previous
Install

Please confirm the following settings before continuing with the installation.

Product name
Encentuate IMS Server

Installation path
C:\Encentuate\IMSServer3.5.51.0

IMS Server fully qualified domain name
IMS.ENCNETWORK.LOCAL

Database server hostname
IMS.ENCNETWORK.LOCAL

Database name
IMSDB

Database user name
USER1

Disk Space Information (for Installation Target):
Required: 238,198,577 bytes
Available: 8,875,360,256 bytes

Summary

⓭ Click Install.

After installation, the IMS Server uses the base connector for Encentuate user validation. The base connector enables any user to sign up as a new Encentuate user providing validation credentials.

To configure Active Directory, see Using the Setup Assistant (IMS Configuration Utility). Complete this task before making the IMS Server available to users for signup.

See Authentication services also for more details.

Upgrading an existing installation of IMS Server

To upgrade the existing IMS Server:

❶ Insert the Encentuate installation CD.

❷ Go to *Start >> Run...*, click **Browse...**, and click **My Computer**. Right-click on the CD drive and select **Explore**.

❸ Click on **imsinstall.exe** icon in the Encentuate installation CD.

❹ InstallAnywhere extracts all the installation fileS.

❺ Verify that you have the required setups, otherwise the installation will not proceed. Click **Next** to continue.

❻ In the next window, select the type of installation to perform.

❼ Choose **Upgrade**. Click **Next** and follow the instructions in the installation wizard.

For IMS Server upgrades, the existing settings (e.g., Java Virtual Machine, concurrent threads, etc.) are not affected. These settings are retained and do have to be reconfigured.

Accessing the IMS Configuration Utility

After installing the IMS Server, the IMSService will automatically start and IMS Configuration Utility will open in your Web browser. You can also click *Start >> Program Files >> Encentuate IMS Server >> IMS Configuration Utility* to open the IMS Configuration Utility. Select **Setup Assistant** to proceed with product activation. For more information, see Using the Setup Assistant.

By default, the IMS Configuration Utility is installed on port 8080, and can be accessed locally from the server console for security reasons (URL: http://imsserver:8080/).

You can also access the IMS Configuration utility using Remote Desktop connection. Run the command: `mstsc /v imsserver`. When connected to the remote server, enter your Administrator user name and password to access the computer. Once you are connected, access the utility through the Windows Start menu.

Integrating with an enterprise’s directory services

An enterprise can have numerous applications deployed on the enterprise network with as many directories to hold user accounts. An infrastructure of that complexity makes it difficult to control audits, enforce policies, and deprovision at the enterprise level. All of these tasks are possible if the enterprise has a single point for collating user accounts.

An enterprise must identify which applications are enterprise applications. Enterprise applications are specific to the business of an enterprise and controlled by an Administrator. For example, Microsoft Windows, Lotus Notes, Active Directory, and other enterprise solutions such as SAP, PeopleSoft, Oracle, and Novell.

One of the enterprise applications will be used for enterprise identity binding. This is required to verify the identities of users who log on using Encentuate Wallet. It also allows for linking the IMS Server with the directory that the enterprise uses to manage their users. Refer to Enterprise identity discussed in IAM Overview for more information on enterprise identity binding.

For example, an enterprise has identified Active Directory for enterprise identity binding as all user account information is stored in Active Directory.

When users register their USB Keys for the first time, they must enter their user name and password for Windows. The IMS Server verifies the identities of users by checking with Active Directory. Once the server receives confirmation, the users can proceed with the registration.

This is possible because certain configurations were made during the installation of the IMS Server, allowing it to communicate with the enterprise's Active Directory.

Currently, the IMS Server supports:

- Active Directory
- LDAP directories

Using the Setup Assistant (IMS Configuration Utility)

After installing the IMS Server, select **Setup Assistant** from the IMS Configuration Utility navigation panel to configure your Active Directory.

For more information on using the Setup Assistant, see Using the Setup Assistant in Using The IMS Configuration Utility.

If Active Directory is not the enterprise directory to be used, go to Basic Settings >> Enterprise Directories in the IMS Configuration Utility. In Enterprise Directories, click Add directory to add a new enterprise directory.

Configuring The IMS Server

You must first set up the IMS server in AccessAdmin before you can add or delete policy templates with the system, machine, or user scope. This chapter discusses how to use AccessAdmin to set up Encentuate IAM.

This chapter covers the following topics:

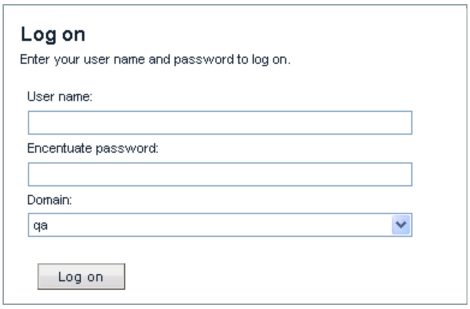
- Specifying IMS Server settings in Setup Assistant (AccessAdmin)
- Configuring policy templates in Setup Assistant (AccessAdmin)

Specifying IMS Server settings in Setup Assistant (AccessAdmin)

Use the Setup Assistant wizard in AccessAdmin to guide you through the setup process.

To specify IMS Server settings in Setup Assistant (AccessAdmin):

1. Launch AccessAdmin (*Start >> All Programs >> Encentuate IMS Server >> Encentuate AccessAdmin*). The Log on page is displayed.



Log on

Enter your user name and password to log on.

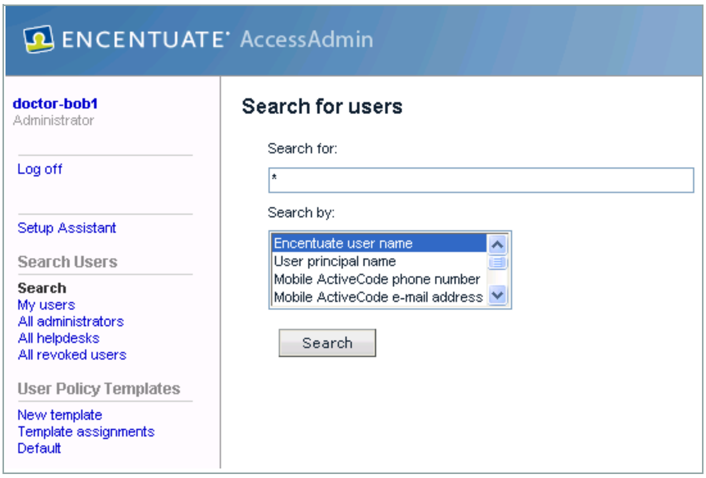
User name:

Encentuate password:

Domain: qa

AccessAdmin logon

2. Enter your logon credentials then click **Log on**. The AccessAdmin page is displayed.



Search for users

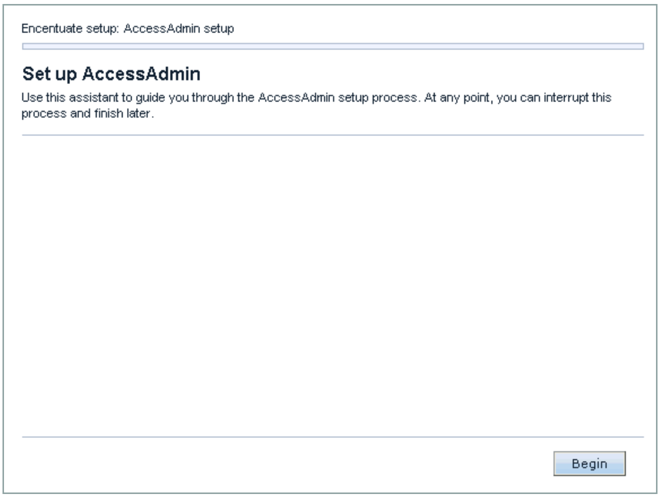
Search for: *

Search by:

- Encentuate user name
- User principal name
- Mobile ActiveCode phone number
- Mobile ActiveCode e-mail address

Search for users

❸ Click **Setup Assistant** from the navigation panel in the AccessAdmin page. The Setup Assistant wizard is displayed.



Encentuate setup: AccessAdmin setup

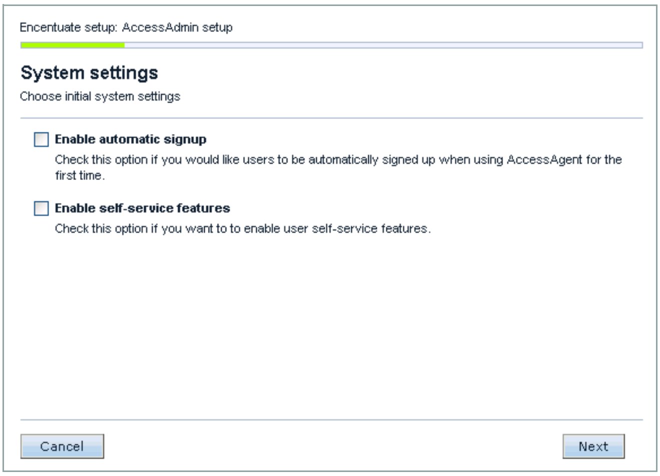
Set up AccessAdmin

Use this assistant to guide you through the AccessAdmin setup process. At any point, you can interrupt this process and finish later.

AccessAdmin Setup Assistant: Begin

❹ Click **Begin** to start setting up AccessAdmin.

❺ Mark the appropriate checkboxes in relation to automatic signup and self-service features, then click **Next**.


Encentuate setup: AccessAdmin setup

System settings

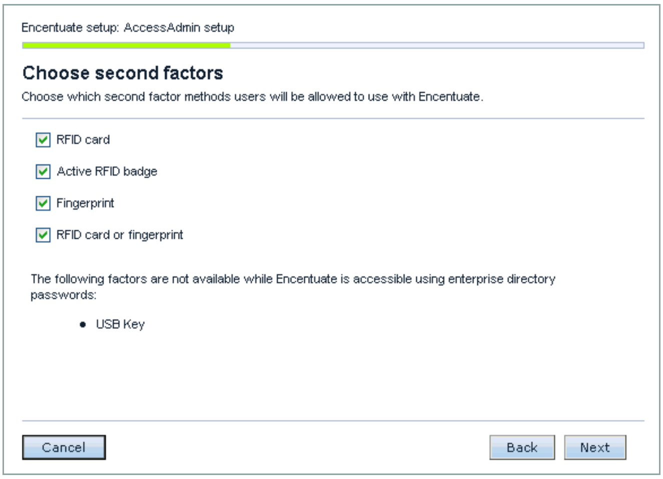
Choose initial system settings

□ **Enable automatic signup**
Check this option if you would like users to be automatically signed up when using AccessAgent for the first time.

□ **Enable self-service features**
Check this option if you want to to enable user self-service features.

AccessAdmin Setup Assistant: System Settings

❻ Choose which second factors your users will be allowed to use in the system. Click **Next**.


Encentuate setup: AccessAdmin setup

Choose second factors

Choose which second factor methods users will be allowed to use with Encentuate.

☑ RFID card

☑ Active RFID badge

☑ Fingerprint

☑ RFID card or fingerprint

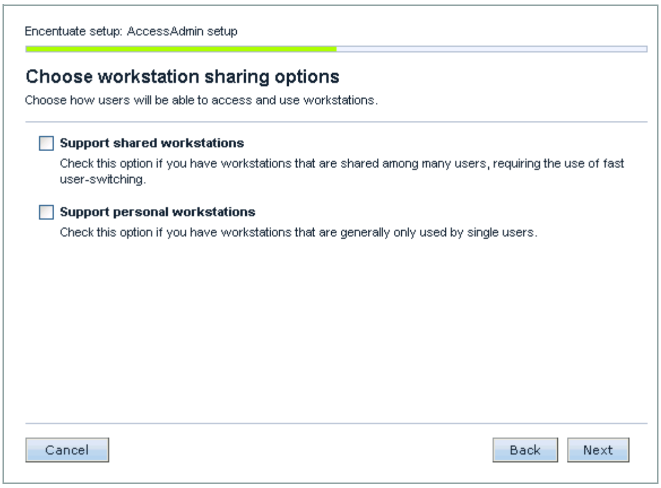
The following factors are not available while Encentuate is accessible using enterprise directory passwords:

- USB Key

AccessAdmin Setup Assistant: Second factors

The USB Key will be included in the set of second factor options if the **Use Active Directory password as Encentuate password** *checkbox is cleared or not selected in the* **Password Synchronization** *screen of the IMS Configuration Utility.*

❼ Choose workstation sharing options. Click **Next**.



Encentuate setup: AccessAdmin setup

Choose workstation sharing options

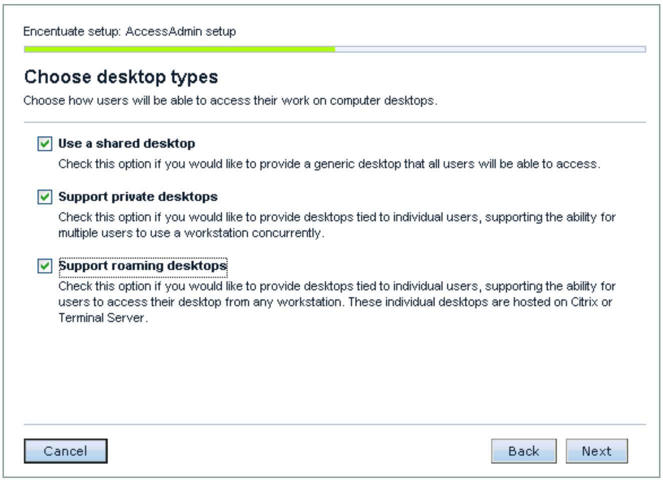
Choose how users will be able to access and use workstations.

□ **Support shared workstations**
Check this option if you have workstations that are shared among many users, requiring the use of fast user-switching.

□ **Support personal workstations**
Check this option if you have workstations that are generally only used by single users.

AccessAdmin Setup Assistant: Workstation sharing

8. Choose desktop types. Click **Next**.



Encentuate setup: AccessAdmin setup

Choose desktop types

Choose how users will be able to access their work on computer desktops.

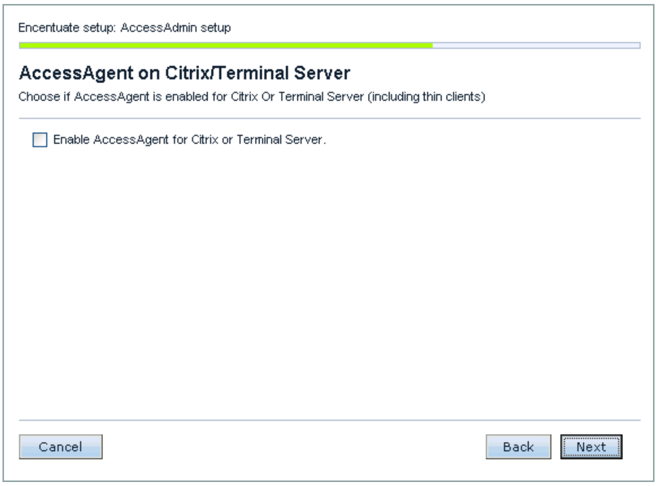
☑ **Use a shared desktop**
Check this option if you would like to provide a generic desktop that all users will be able to access.

☑ **Support private desktops**
Check this option if you would like to provide desktops tied to individual users, supporting the ability for multiple users to use a workstation concurrently.

☑ **Support roaming desktops**
Check this option if you would like to provide desktops tied to individual users, supporting the ability for users to access their desktop from any workstation. These individual desktops are hosted on Citrix or Terminal Server.

AccessAdmin Setup Assistant: Desktop types

9. Mark the **Enable AccessAgent for Citrix or Terminal Server** checkbox to allow AccessAgent to run on the Citrix or terminal server that your system supports. Click **Next**.



Encentuate setup: AccessAdmin setup

AccessAgent on Citrix/Terminal Server

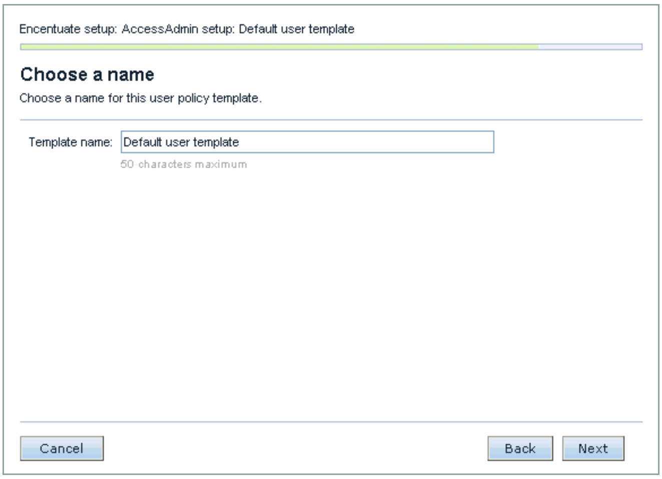
Choose if AccessAgent is enabled for Citrix Or Terminal Server (including thin clients)

□ Enable AccessAgent for Citrix or Terminal Server.

AccessAdmin Setup Assistant: Citrix/Terminal Server

⑩ Enter a name for the default user policy template.The default user policy template is applied to users if there are no existing policy templates applied to them.

Click **Next**.



Encentuate setup: AccessAdmin setup: Default user template

Choose a name

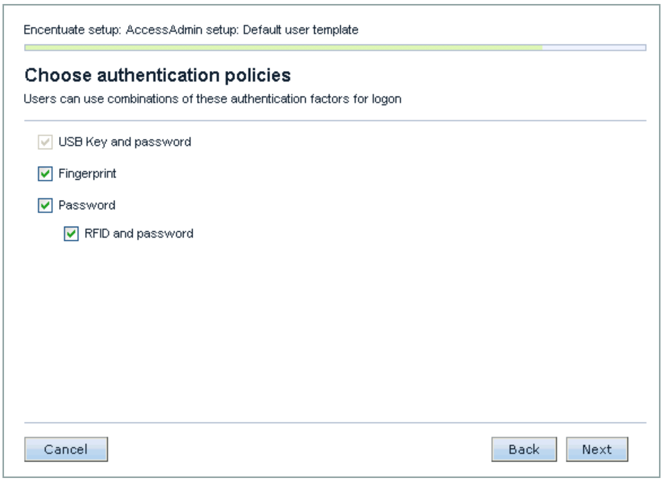
Choose a name for this user policy template.

Template name: Default user template

50 characters maximum

AccessAdmin Setup Assistant: Template Name

⑪ Choose from a list of authentication policies that will be applied to all users. Click **Next**.



Encentuate setup: AccessAdmin setup: Default user template

Choose authentication policies

Users can use combinations of these authentication factors for logon

☑ USB Key and password

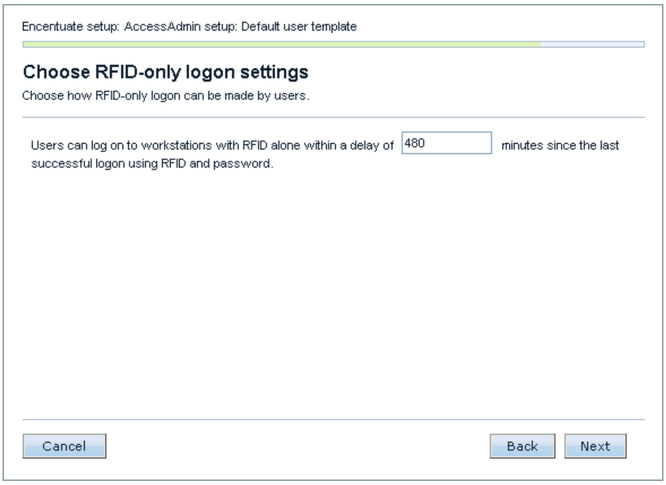
☑ Fingerprint

☑ Password

☑ RFID and password

AccessAdmin Setup Assistant: Authentication policies

⓬ Enter the time delay value in minutes. If the user logs on again on the workstation beyond the set time delay, the system will prompt the user to log on with both the RFID and password. Otherwise, the user only needs to tap the RFID to log on again within the set time frame.



Encentuate setup: AccessAdmin setup: Default user template

Choose RFID-only logon settings

Choose how RFID-only logon can be made by users.

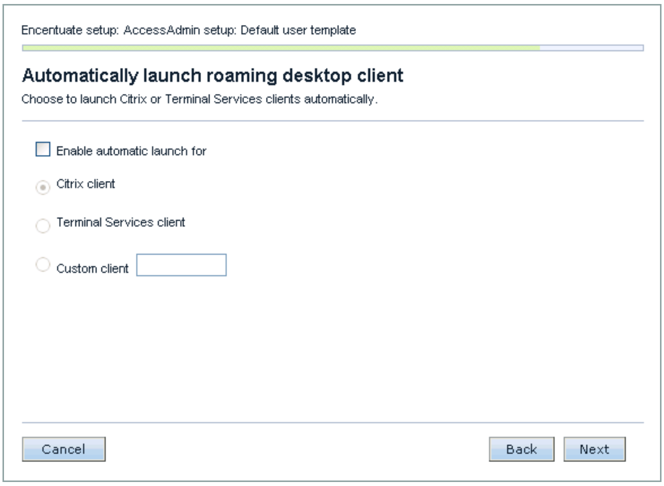
Users can log on to workstations with RFID alone within a delay of 480 minutes since the last successful logon using RFID and password.

AccessAdmin Setup Assistant: RFID logon settings

This setting works across machines, even on a roaming setup.

⓭ For roaming desktop users, mark the **Enable automatic launch for** checkbox, then select the client type your users need to launch automatically. Click **Next**.

This setting is only required on a roaming setup.



Encentuate setup: AccessAdmin setup: Default user template

Automatically launch roaming desktop client

Choose to launch Citrix or Terminal Services clients automatically.

□ Enable automatic launch for

● Citrix client

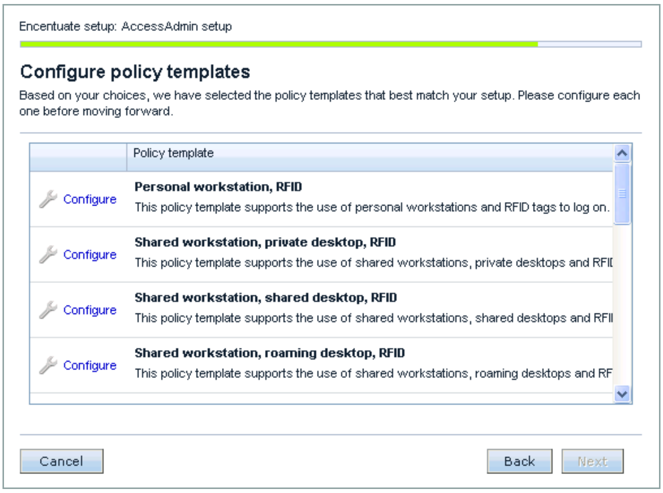
○ Terminal Services client

○ Custom client

AccessAdmin Setup Assistant: Roaming desktop client

⓮ Click **Configure** to set up each policy template. Click **Next** once you are done setting up all of the templates.

The templates in the Policy Template table are auto-generated based on the previously selected options in Setup Assistant.



Encentuate setup: AccessAdmin setup

Configure policy templates

Based on your choices, we have selected the policy templates that best match your setup. Please configure each one before moving forward.

	Policy template
Configure	**Personal workstation, RFID** This policy template supports the use of personal workstations and RFID tags to log on.
Configure	**Shared workstation, private desktop, RFID** This policy template supports the use of shared workstations, private desktops and RFI
Configure	**Shared workstation, shared desktop, RFID** This policy template supports the use of shared workstations, shared desktops and RFI
Configure	**Shared workstation, roaming desktop, RFID** This policy template supports the use of shared workstations, roaming desktops and RF

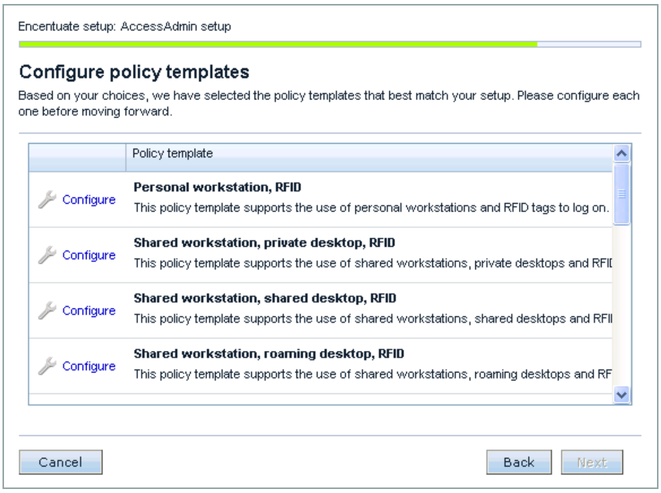
AccessAdmin Setup Assistant: Configure policy templates (1/3)

Configuring policy templates in Setup Assistant (AccessAdmin)

Use AccessAdmin's Setup Assistant to set up user and machine policy templates. The policy templates in this wizard are auto-generated based on previously-selected options in the Setup Assistant.

To configure policy templates in Setup Assistant (AccessAdmin):

❶ Click the **Configure** link of the policy template you need to configure.



Encentuate setup: AccessAdmin setup

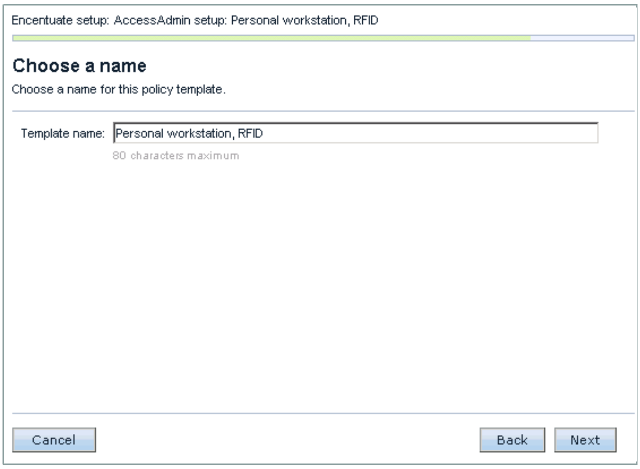
Configure policy templates

Based on your choices, we have selected the policy templates that best match your setup. Please configure each one before moving forward.

	Policy template
Configure	**Personal workstation, RFID** This policy template supports the use of personal workstations and RFID tags to log on.
Configure	**Shared workstation, private desktop, RFID** This policy template supports the use of shared workstations, private desktops and RFII
Configure	**Shared workstation, shared desktop, RFID** This policy template supports the use of shared workstations, shared desktops and RFII
Configure	**Shared workstation, roaming desktop, RFID** This policy template supports the use of shared workstations, roaming desktops and RF

AccessAdmin Setup Assistant: Configure policy templates (2/3)

❷ Enter a name for the policy template, and click **Next**.



Encentuate setup: AccessAdmin setup: Personal workstation, RFID

Choose a name

Choose a name for this policy template.

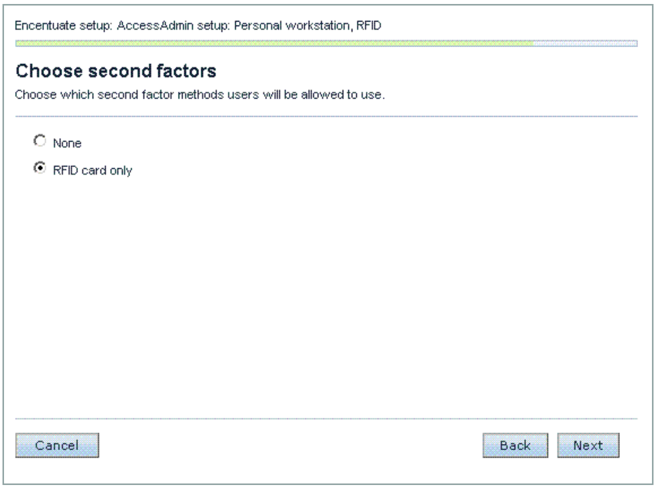
Template name: Personal workstation, RFID

80 characters maximum

AccessAdmin Setup Assistant: Configure policy templates (3/3)

❸ Select the authentication factor to use, depending on the authentication factors supported on machines assigned to this policy template. Click **Next**.

The **RFID card only** option allows the user to logon using his RFID. It also allows the user to unlock the workstation by just an RFID tap if it is done within the set time delay.



Encentuate setup: AccessAdmin setup: Personal workstation, RFID

Choose second factors

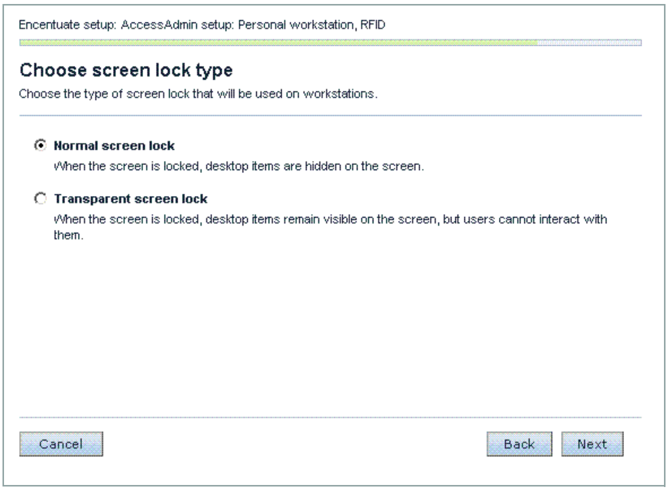
Choose which second factor methods users will be allowed to use.

○ None

● RFID card only

AccessAdmin Setup Assistant: Personal workstation RFID (1/5)

❹ Select the screen lock type to be used on workstations. Click **Next**.



Encentuate setup: AccessAdmin setup: Personal workstation, RFID

Choose screen lock type

Choose the type of screen lock that will be used on workstations.

● **Normal screen lock**
When the screen is locked, desktop items are hidden on the screen.

○ **Transparent screen lock**
When the screen is locked, desktop items remain visible on the screen, but users cannot interact with them.

AccessAdmin Setup Assistant: Personal workstation RFID (2/5)

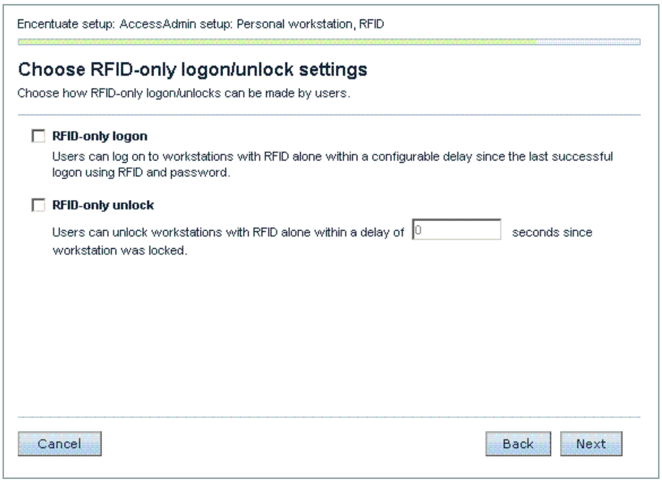
❺ Choose how RFID-only logon /unlock settings can be made by users, if applicable. If you choose **RFID-only logon,** see Specifying IMS Server settings in Setup Assistant (AccessAdmin), step 12, for time-delay settings.

Enter the time delay value in seconds if you select the **RFID-only unlock** option.

RFID-only logon *works across machines. You can unlock from another machine in a roaming setup by tapping your RFID within a set time delay. You need to provide your password only if you attempt to unlock your machine beyond the pre-set time delay.*

RFID-only unlock *works only on the same machine. If you attempt to unlock from another machine in a roaming setup, the system will prompt you to tap your RFID and provide your password.*

Click **Next**.



Encentuate setup: AccessAdmin setup: Personal workstation, RFID

Choose RFID-only logon/unlock settings

Choose how RFID-only logon/unlocks can be made by users.

☐ RFID-only logon

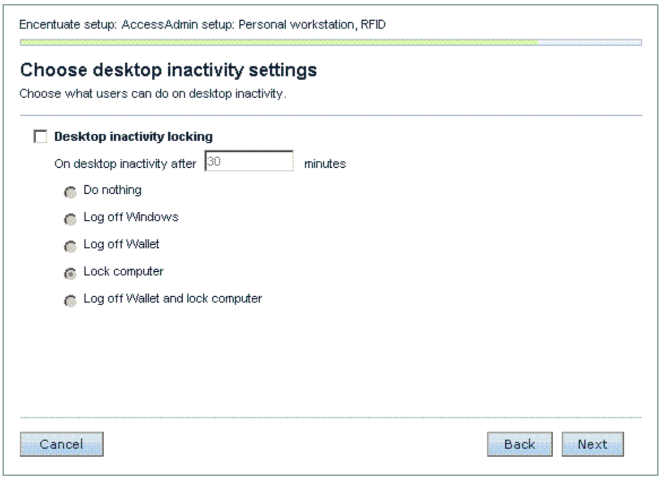
Users can log on to workstations with RFID alone within a configurable delay since the last successful logon using RFID and password.

☐ RFID-only unlock

Users can unlock workstations with RFID alone within a delay of [0] seconds since workstation was locked.

AccessAdmin Setup Assistant: Personal workstation RFID (3/5)

6. Choose the appropriate desktop inactivity option. Click **Next**.



Encentuate setup: AccessAdmin setup: Personal workstation, RFID

Choose desktop inactivity settings

Choose what users can do on desktop inactivity.

☐ Desktop inactivity locking

On desktop inactivity after [30] minutes

○ Do nothing

○ Log off Windows

○ Log off Wallet

● Lock computer

○ Log off Wallet and lock computer

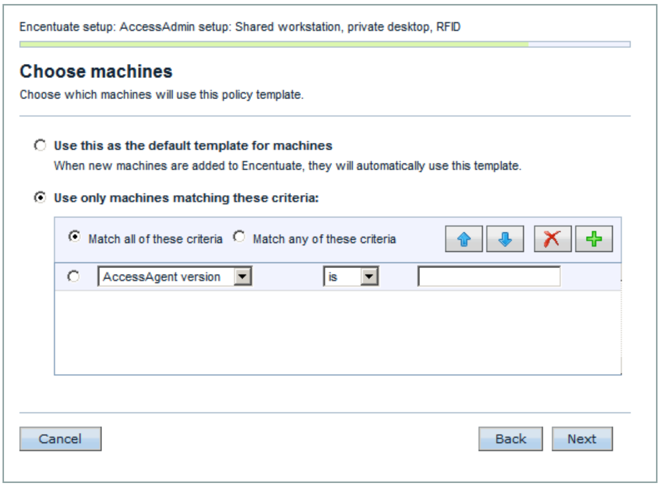
AccessAdmin Setup Assistant: Personal workstation RFID (4/5)

7. You can use this as the default templates for machines or use the template for specific machines that meets a set of criteria.

   Select either **Match all of these criteria** or **Match any of these criteria** as filters.

   Specify more detailed criteria by selecting from the drop-down menu. For more information on specifying criteria, see Searching and managing machines, To set criteria:.

   Click **Next**.



Encentuate setup: AccessAdmin setup: Shared workstation, private desktop, RFID

Choose machines

Choose which machines will use this policy template.

○ **Use this as the default template for machines**

When new machines are added to Encentuate, they will automatically use this template.

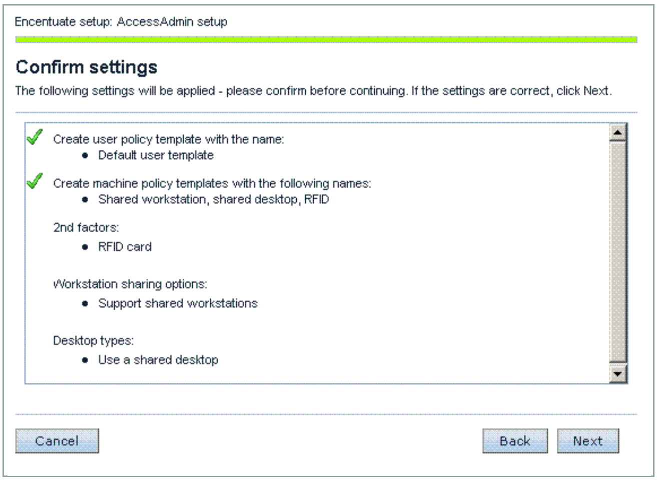
● **Use only machines matching these criteria:**

● Match all of these criteria ○ Match any of these criteria

○ AccessAgent version ▾ is ▾

AccessAdmin Setup Assistant: Personal workstation RFID (5/5)

8. Confirm the settings you have applied and click **Next**.



Encentuate setup: AccessAdmin setup

Confirm settings

The following settings will be applied - please confirm before continuing. If the settings are correct, click Next.

✓ Create user policy template with the name:
- Default user template

✓ Create machine policy templates with the following names:
- Shared workstation, shared desktop, RFID

2nd factors:
- RFID card

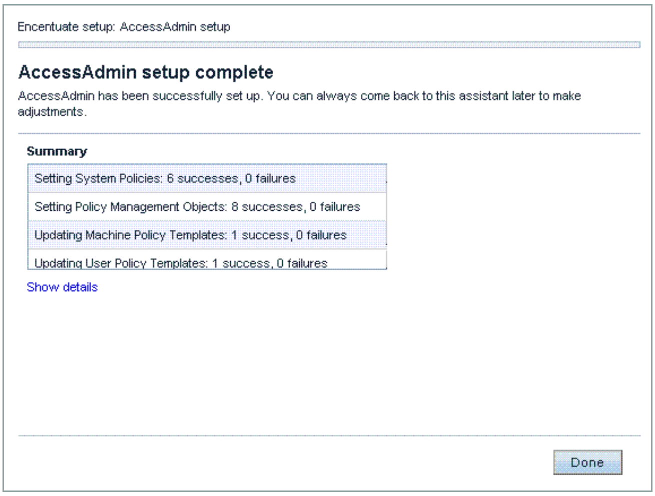
Workstation sharing options:
- Support shared workstations

Desktop types:
- Use a shared desktop

AccessAdmin Setup Assistant: Confirm settings

9. A summary of configuration results indicates a successful setup. Click **Show details** for a detailed list of the settings you have applied on the policy template. Click **Done**.

This summary page will not be displayed until all the policy templates are configured. Click Back to return to the previous pages in the wizard to configure all policy templates.



Encentuate setup: AccessAdmin setup

AccessAdmin setup complete

AccessAdmin has been successfully set up. You can always come back to this assistant later to make adjustments.

Summary

Setting System Policies: 6 successes, 0 failures

Setting Policy Management Objects: 8 successes, 0 failures

Updating Machine Policy Templates: 1 success, 0 failures

Updating User Policy Templates: 1 success, 0 failures

AccessAdmin Setup Assistant: Setup complete

Installing AccessAgent

You can install Encentuate AccessAgent using an Encentuate USB Key or Encentuate AccessAgent installation CD. You do not have to install AccessAgent on the same computer where the IMS Server is installed. Use any of the three enterprise identities you specified during installation of the IMS Server.

This will allow you to access the IMS Server and log on to AccessAdmin. When logging on to AccessAdmin, enter the fully qualified domain name (for example, https://ims.encentuate.com.).

✓ *A common problem when installing AccessAgent on the server (in particular, Windows 2003 Server) is that Windows has an advanced security option enabled by default. This option prevents AccessAgent from performing authentication with IMS Server, hence the user cannot use AccessAdmin.*

To disable this option, go to Start >> Control Panel >> Add/remove programs >> Windows components and uninstall **Advanced Security Option**.

This chapter covers the following topics:

- Installer options
- Push installation
- Manual installation
- Setting the IMS Server location
- Program folders
- Registry entries

Installer options

The AccessAgent installer consists of the following:

- **AccessAgent.msi**

  No **setup.exe** is present, instead, only the MSI installer is provided.

You do not have to uninstall your previous version AccessAgent, if any, before installing a new version.

- Config folder

  The Config folder should contain the following:

  DeploymentScript.vbs

  This must be installed/executed. If DeploymentScript.vbs is used, make sure the VBScript contains the following:

  - sub PostCopy()
  - end sub
  - sub PreRemove()
  - end sub

  The script will be called after all the files have been transferred and registry has been written.

  SetupHlp.ini

  This provides options to be used during installation. The options provided in SetupHlp.ini are divided into 4 categories:

  1. Setup time only options

     Options that cannot be changed after installation.

Option Name	Value	Description
EnginaEnabled	1 | 0 (default: 1)	Whether to replace current GINA with EnGINA. *The behavior of this option is consistent for workstations, Terminal Servers, and Citrix servers. For Citrix servers, option 0 is recommended.*
RebootEnabled	1 | 0 (default: 1)	Whether to trigger a machine reboot after setup.
RebootConfirmationEnabled	1 | 0 (default: 1)	Whether to confirm with user before rebooting.Effective only if RebootEnabled=1.

Setup time only options

Option Name	Value	Description
EnginaConflict-PromptEnabled	1 | 0 (default: 1)	In case of GINA conflict, whether a prompt should be displayed.
UsbKeyPromptEnabled	1 | 0 (default: 1)	Whether to prompt user to insert USB Key, if it is not already inserted during installation time.
ImsConfiguration-Enabled	1 | 0 (default: 1)	Whether to configure default IMS Server settings and install certificates from that server during setup.
ImsConfiguration-PromptEnabled	1 | 0 (default: 0)	Whether to prompt user for the default IMS Server entry even if it is already correctly configured.Effective only if ImsConfigurationEnabled=1.
WalletCacheRemovedOnUpgrade	1 | 0 (default: 0)	Whether to remove cached Wallets on an upgrade.
InstallTypeGpo	1 | 0 (default: 0)	Whether to suppress all prompts and write to log. Required for AD GPO installation.
EncentuateRegistryRemovalEnabled	1 | 0 (default: 0)	Whether the Encentuate registry entries should be cleared after AccessAgent is uninstalled.
UsbKeyUtilityInstallationEnabled	1 | 0 (default: 0)	Whether to install the USB Key Utility when AccessAgent is installed.
EncentuateNetworkProviderEnabled	1 | 0 (default: 0)	Whether to enable the installation of Encentuate Network Provider during AccessAgent installation.
JVMInstallationDirectories	See description	Directories containing JVMs for which to enable Java automatic sign-on support. Each directory is to be separated by a vertical bar. No space is allowed between two JVM directories. For example, “C:\Program Files\Java\ jre1.5.0_11|C:\Encentuate\ j2re1.4.1”

Setup time only options

2. Setup time and runtime options that map to multiple registry values each

Options that can be changed after installation (by modifying registry values), and each is mapped to several registry values.

Option Name	Value	Description
ImsSecurePortDefault	default: 443	Default download port number for the default IMS Server.
ImsDownloadPortDefault	default: 80	Default download port number for the default IMS Server.
ImsDownloadProtocolDefault	default: http://	Default download protocol for the default IMS Server.

Setup time and runtime options that map to multiple registry values each

3. Setup time and runtime options that map to one registry value each

   Options that can be changed after installation (by modifying registry values), and each is mapped to one registry value.

Option Name	Value	Description
WalletTypeSupported	0: IMS only 1: Non-IMS only 2: Both IMS and non-IMS (default: 0)	Supported Wallet types.
ImsAddressPromptEnabled	1 | 0 (default: 1)	Whether to prompt user for IMS address during sign up, even if the IMS address specified in ImsServerName is correct.
✱ ImsServerName	IMS Server hostname	Default IMS Server name.

Setup time and runtime options that map to one registry value each

In a typical setup, only IMsServerName needs to be set.

4. Dependency URLs

   URLs that installer directs user to if certain components required for installation are missing, for example, High Encryption Pack.

Other files

Any other file (for example, logon_banner.bmp) to be copied to the Encentuate program files folder.

Uninstaller will not remove these copied files. These files will also not be repaired by the installer.

- Reg folder

  The Reg folder should contain the DeploymentOptions.reg, which will be merged into the Windows registry.

  Any other file will be ignored.

Push installation

The package of AccessAgent.msi file, and Config and Reg folders, can be centrally pushed out to client machines using software deployment tools, like AD GPO or Microsoft Systems Management Server (SMS).

For certain push installations, it may be necessary to set the installer path in the AccessAgent.msi file, as follows:

- Open the AccessAgent.msi file using Orca editor (part of Windows Installer SDK).
- Click on the Property table on the left.
- Set CONFIG_PARAMS_BASE_PATH to the desired path.

For deployment via SMS, especially during an upgrade, a VBScript can be written to present users with prompts such as:

```
You cannot use AccessAgent during the upgrade, (for example,
Single Sign-on to applications, will be temporarily disabled).
Restart the system when the upgrade is completed.
```

This VBScript can then execute AccessAgent.msi, with switches to suppress AccessAgent installer prompts (AccessAgent.msi /q /norestart /l*v C:\AccessAgent.Log).

To allow the VBScript to interact with the user with prompts, open Program Properties dialog box and go to the Environment tab. In Run mode, make sure that Allow users to interact with this program is marked.

Manual installation

Once you place the AccessAgent installation CD in your CD drive, the installation will automatically begin. If installation does not begin, access the CD using Windows Explorer and double-click `AccessAgent.msi`.

The installation files for AccessAgent can also be placed in the storage area of the Encentuate USB Key and you can install AccessAgent from the USB Key. Insert the USB Key into the port, and access the key using Windows Explorer. Double-click on `AccessAgent.msi` to start the installer.

Setting the IMS Server location

Set the location of the IMS Server by setting the ImsServerName key in **SetupHlp.ini**. The AccessAgent installer will automatically download the IMS Server certificate from the IMS Server.

If the certificate download fails during installation, the user will see a prompt and will determine whether to still proceed with the installation. However, the user cannot sign up or log on unless the user successfully downloads the certificate.

This can be done by running *Start >> All Programs >> Encentuate AccessAgent >> Set IMS Server Location*. Alternatively, you can also run the file from this location **C:\Program Files\Encentuate\SetupCertDlg.exe**.

The Set IMS Server Location utility currently does not allow users to modify the IMS Server name and port number. These must be modified by setting the registry entries that correspond to the appropriate machine policies: **pid_ims_server_name** and **pid_ims_download_service_port**.

Program folders

AccessAgent program files and data are stored, by default, within the **C:\Program Files\Encentuate** folder.

Program files: C:\Program Files\Encentuate

Logs: C:\Program Files\Encentuate\logs

User and machine Wallets (hidden files): C:\Program Files\Encentuate\Cryptoboxes

To see the Wallet files, make sure that Windows explorer has been configured to Show hidden files and folders.

The machine Wallet (**C:\Program Files\Encentuate\Cryptoboxes\Wallets\machine.wlt**) contains system policies and AccessProfiles downloaded from the current IMS Server. It is downloaded from the IMS Server during the first startup after installation.

If the download of the machine Wallet is unsuccessful at startup, the synchronizer retries every 20 seconds for 5 times. After these 5 times, if downloading is still unsuccessful, the synchronizer will retry at intervals of 2 minutes until it is successful.

✓ *By default, AccessAgent is installed to* C:\Program Files\Encentuate. *Ensure that C: drive is present.*

Registry entries

AccessAgent registry entries are stored in the [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate] key. Default registry values are automatically populated upon installation.

✓ *The Administrator sets and manages the machine policies in AccessAdmin.*

Advanced configuration parameters are specified through registry values that are grouped under the appropriate registry keys according to the following convention:

Registry Key	Type of Policy
[Encentuate/DeploymentOptions]	All non-IMS machine policies
[Encentuate/IMSService/Default-IMSService]	Policies related to the default IMS Server
[Encentuate/IMSService/Global-IMSService]	URLs to SOAP services provided by the IMS Server
[Encentuate/AccessAgent/Integration]	Settings related to integration with non-Encentuate software
[Encentuate/Temp]	Temporary registry values for development and troubleshooting purposes (these policies are not officially supported and should not be used for actual deployment)

Maintaining The IMS Server

Maintaining the IMS Server is a task that the Administrator needs to perform periodically, to ensure that data is backed up, logs are created, and that the IMS Server is running smoothly. In this section, you can find out about how to back up the IMS Server database, how to view logs, and how to perform system diagnostics.

This chapter covers the following topics:

- The Encentuate IMS Server architecture
- About services and modules
- Backing up the database
- Viewing logs
- Starting the IMS Server
- Stopping the IMS Server
- Checking the IMS Server status and version
- Sending feedback to Encentuate
- Getting help

The Encentuate IMS Server architecture

The IMS Server is the central repository where identity information is consolidated. It works with the AccessAgents that are distributed across the network to provide single sign-on to users. It also allows an enterprise to incrementally transit users from password-based authentication to certificate-based authentication, allowing for strong digital identity.

The IMS Server is written in Java and runs on a Java application server. The application server used is Apache Tomcat (Tomcat).

The IMS Server uses Simple Object Access Protocol (SOAP) to communicate with AccessAgent. Java Server Pages are used to control the appearance and content of AccessAdmin.

A certificate authority is subsumed in the IMS Server and it uses a relational database management system (RDBMS) as its internal data store. Currently the RDBMS supported are Microsoft SQL Server, MSDE (Microsoft SQL Server 2000 Desktop Engine), and Oracle 9i. However, other RDBMS will be supported in the near future.

About services and modules

On a macro level, the IMS Server provides a central location for administration of user identities, policy definition, policy enforcement and collation of audit trails. From the back-end, it provides certification, synchronization and backup services to the AccessAgents distributed across the network, and other components such as Encentuate IAM Application Connectors and Encentuate IAM Authentication Bridges.

Encentuate password, authentication factors, and Encentuate AccessAgent are components that work closely with Encentuate IMS Server. Other components, such as Encentuate IAM Application Connectors, Encentuate IAM Authentication Bridges and Encentuate Signature HSM allow the IMS Server to provide and enforce strong digital identity.

Application Connectors enable the IMS Server to connect to applications in an enterprise and invoke services. The IMS Server publishes a fixed application program interface (API) for the development of Application Connectors. This API allows easy and quick development of new connectors and is currently expressed as Java and SOAP interfaces.

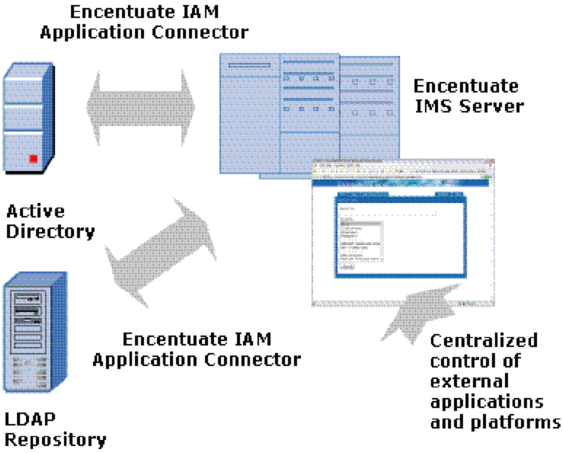
Encentuate IMS Bridges extend functionalities of third party programs, allowing them to communicate with the IMS. IMS Service Modules, on the other hand, extend the functionalities of the IMS Server itself. Examples include IMS Bridges that provide OTP and certificate-based authentication services for applications.

Application connectors

Application Connectors provide a framework for integrating with different applications extending the capability of the IMS Server. Connectors enable an enterprise to integrate all of its applications with Encentuate IMS Server, creating a single point from where user identities can be managed.

In its simplest form, a Connector is a module within the IMS Server that communicates with an external application to perform user management and provisioning operations. These operations include looking up user information, verifying and changing passwords, and disabling user accounts.

The underlying architecture of Application Connectors allow them to be flexible and extensible. All Application Connectors adhere to a standard interface making it easy to add arbitrary connectors without making changes in the IMS Server. Depending on the requirements of an enterprise, Application Connectors can also be implemented as a subset of the full interface.


Encentuate IAM Application Connector
Encentuate IMS Server
Active Directory
Encentuate IAM Application Connector
Centralized control of external applications and platforms
LDAP Repository

Application Connectors

Deployment of an Application Connector requires configuring the connector so it can communicate with the application. Communication happens via the protocol that the application supports. Applications such as LDAP user directories and web applications are easy to configure since they are based on industry standards.

Applications that use proprietary communication protocols requires liaising directly with software vendors to see how LDAP user directories can be configured to communicate with their applications.

The following Application Connectors are available:

- Active Directory Connector
- ADSI Connector
- NIS Connector
- Web applications
- Windows NT Connector
- JDE OneWorld Web Connector
- Oracle 11i E-business Suite Connector

Management tools

The IMS Server is designed to require minimal management or maintenance. Any maintenance efforts can be done using AccessAdmin or IMS Configuration Utility.

Backing up the database

Data is essential for an enterprise's day-to-day operations, and there should be backup and restore plans in place. There as so many ways data loss can occur (for example, accidental deletion of important data, corruption of data critical to daily operations, and natural disasters can take us by surprise and cause havoc).

Backup and restore plans allow you to recover data and minimize business and operation down-time. Without implementing backup and recovery plans, critical data may not be retrieved.

Backup and restore plans must be based on the importance of data, how often data is used and updated, how fast data should be restored, and the equipment that will be used to perform backup and similar factors.

Backup and restore plans should come about after careful planning and considering the impact of data in your enterprise. Your database Administrator should be responsible for overlooking the whole operation.

The IMS Server database is critical for day-to-day operations. It contains global policies, configurations required for the IMS Server, and user information which is constantly synchronized. It is advised to use the same backup and recovery strategy for other critical data.

The plans should dictate the backup frequency and the media which will be used for backup. Back up the entire IMS Server database rather than specific tables.

The following are some useful links:

- How to manage the Microsoft SQL Server Desktop Engine (MSDE 2000) by using the OSQL utility

  This article describes how to use OSQL to manage and backup a MSDE database.

  http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B325003#12

- MSDE Backup using products such as Ultrabac, ArcServe and Backup Exec

  http://www.securewave.com/support/tech_notes.html

- Customizing a MSDE or SQL Server Installation http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q233/3/12.ASP&NoWebContent=1

Schedule the backing up of the IMS Server Database using the Backup Parameters in the Encentuate IMS Server configuration file (**ims.xml**). See IMS Server housekeeping for details of the backup parameters you must set.

Viewing logs

There are three types of logs available in the IMS Server: user, system, and Administrator logs. The user log contains information about actions performed by the user. System logs provide information related to the IMS Server, while Administrator logs list Helpdesk officer and Administrator actions.

User logs are available to both Helpdesk officer and Administrator, though it is likely that the Helpdesk officer will be going through these logs. Only the Administrator has access to the system and Administrator logs.

The events that appear in AccessAdmin are specified in the configuration file. These configurations are specified by the professional services during deployment of Encentuate IAM. These settings can be modified at a later time to meet changing needs of an enterprise. Refer to Using The IMS Configuration Utility to learn how to configure what appears in the different logs.

All information is stored in the database. An enterprise can access the information and use it to integrate with report generation software such as Crystal Reports, Oracle Reports, Elixir Reports and the like to come up with variety of reports that sort information in a more readable and visual form.

Starting the IMS Server

Start the IMS Server by going to *Start >> Programs >> Encentuate IMS Server* and clicking **Start IMS Service**. Alternatively you can type:

```
net.exe start IMSService or imsserver\ims\bin\runserver
```

at the command prompt to start the server.

To verify that you can use AccessAdmin: Go to https://`hostname`

Here, *hostname* is the name of the computer on which the IMS Server is installed.

If you start the IMS Server using the command prompt, the IMS Server will not run as a service. Thus, if the session which started the console is closed, the IMS Server will also be stopped.

Stopping the IMS Server

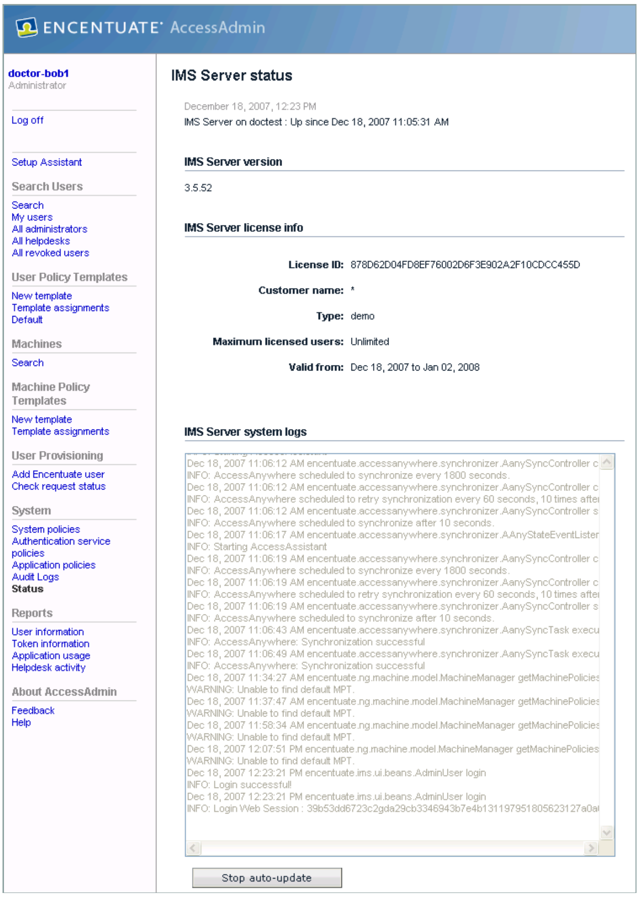
Stop Encentuate IMS Server by going to *Start >> Programs >> Encentuate IMS Server* and clicking **Stop IMS Service**. Alternatively you can run:

```
net.exe stop IMSService
```

at the command prompt to stop the server.

Checking the IMS Server status and version

In the AccessAdmin navigation panel, select *System >> Status* to view the system status: the server availability and version number. You can also view IMS server system logs in real-time, including start and stop the auto-update to copy the log.



IMS Server status

December 18, 2007, 12:23 PM
IMS Server on doctest : Up since Dec 18, 2007 11:05:31 AM

IMS Server version

3.5.52

IMS Server license info

License ID:	878D62D04FD8EF76002D6F3E902A2F10CDCC455D
Customer name:	*
Type:	demo
Maximum licensed users:	Unlimited
Valid from:	Dec 18, 2007 to Jan 02, 2008

IMS Server system logs

```
Dec 18, 2007 11:06:12 AM encentuate.accessanywhere.synchronizer.AanySyncController c
INFO: AccessAnywhere scheduled to synchronize every 1800 seconds.
Dec 18, 2007 11:06:12 AM encentuate.accessanywhere.synchronizer.AanySyncController c
INFO: AccessAnywhere scheduled to retry synchronization every 60 seconds, 10 times afte
Dec 18, 2007 11:06:12 AM encentuate.accessanywhere.synchronizer.AanySyncController s
INFO: AccessAnywhere scheduled to synchronize after 10 seconds.
Dec 18, 2007 11:06:17 AM encentuate.accessanywhere.synchronizer.AAnyStateEventLister
INFO: Starting AccessAssistant
Dec 18, 2007 11:06:19 AM encentuate.accessanywhere.synchronizer.AanySyncController c
INFO: AccessAnywhere scheduled to synchronize every 1800 seconds.
Dec 18, 2007 11:06:19 AM encentuate.accessanywhere.synchronizer.AanySyncController c
INFO: AccessAnywhere scheduled to retry synchronization every 60 seconds, 10 times afte
Dec 18, 2007 11:06:19 AM encentuate.accessanywhere.synchronizer.AanySyncController s
INFO: AccessAnywhere scheduled to synchronize after 10 seconds.
Dec 18, 2007 11:06:43 AM encentuate.accessanywhere.synchronizer.AanySyncTask execu
INFO: AccessAnywhere: Synchronization successful
Dec 18, 2007 11:06:49 AM encentuate.accessanywhere.synchronizer.AanySyncTask execu
INFO: AccessAnywhere: Synchronization successful
Dec 18, 2007 11:34:27 AM encentuate.ng.machine.model.MachineManager getMachinePolicies
WARNING: Unable to find default MPT.
Dec 18, 2007 11:37:47 AM encentuate.ng.machine.model.MachineManager getMachinePolicies
WARNING: Unable to find default MPT.
Dec 18, 2007 11:58:34 AM encentuate.ng.machine.model.MachineManager getMachinePolicies
WARNING: Unable to find default MPT.
Dec 18, 2007 12:07:51 PM encentuate.ng.machine.model.MachineManager getMachinePolicies
WARNING: Unable to find default MPT.
Dec 18, 2007 12:23:21 PM encentuate.ims.ui.beans.AdminUser login
INFO: Login successful!
Dec 18, 2007 12:23:21 PM encentuate.ims.ui.beans.AdminUser login
INFO: Login Web Session : 39b53dd6723c2gda29cb3346943b7e4b1311979518056231 27a0a
```

Viewing system status

Sending feedback to Encentuate

If you have thoughts about Encentuate IMS Server user interface or have questions that are not covered in this guide, you can use the **Feedback** link in the AccessAdmin navigation panel.

You also return to the Feedback panel if an unexpected error occurs while you are using Encentuate IMS Server's user interface.

You are not required to enter your e-mail address, but you can do so if you wish. This way, Encentuate can keep you informed of the progress of solving your problem. Enter your comments and click Send.

Getting help

If you require help while you are using the Encentuate IMS Server user interface, click the **Help** in the AccessAdmin navigation panel. The contents of Encentuate IAM Helpdesk Guide appear here. You will be taken to the relevant section when you click on a topic.

Click *AccessAdmin* >> *About AccessAdmin* >> *Help* and find the topic that you are need information about from among the listed topics.

Searching and Managing Users

This section discusses how to manage users with Encentuate AccessAdmin. There are two ways to log on to AccessAdmin:

- Go to the console of the machine where the IMS Server is installed, access https://imsservername, and a logon prompt will be presented; or

- Log on to AccessAgent on any machine as Administrator, and then launch https://imsservername.

When logging on to AccessAdmin, enter the fully qualified domain name (for example, https://ims.encentuate.com).

If the IMS server is accessed without using the fully qualified domain name, AccessAgent will not be able to perform logon to search page automatically.

In the main user interface, you can find links to all the available administration functions. The main link, AccessAdmin, should be visible at all times. Click the link to view the AccessAdmin user interface.

As an Administrator, here are the tasks you can perform using AccessAdmin:

- Searching for users

- Viewing and editing user settings

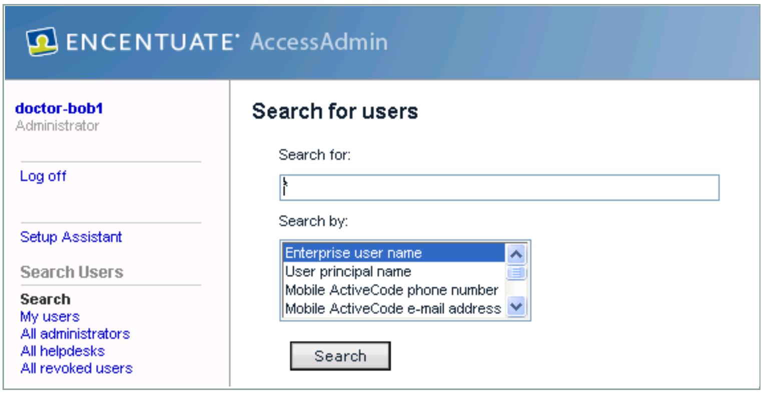
Searching for users

There are many ways you can search for users in AccessAdmin. You can search for a single user, a group of users, or users that have been assigned to you. Once you have located the users, you can view and modify their settings.

Conducting a new search

To conduct a new search:

1. Click on *AccessAdmin >> Search users >> New search*.



New search

2. Enter the subject of your search in **Search for.**

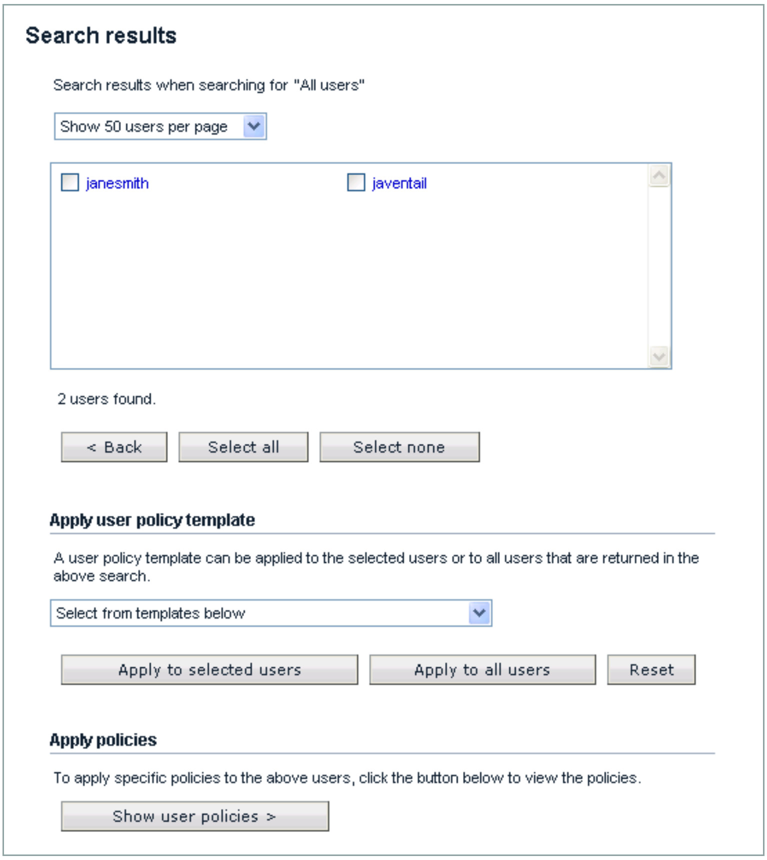
You can make a partial search followed by an asterisk (*) to find partially matching results. For example, if you want to find all users whose enterprise user name begin with the letter “i“, enter “i“ in the Search for field.*

3. Select a search criteria from the **Search by** list.

4. Click **Search**. The search results are displayed, containing all the matches or partial matches.

   You can also make a partial search—for example, if you want to find all users whose names start with the letter A, you can type **A*** in the **Search for** field.

   The matching result will appear on the screen. If you see the user that you are looking for, click on the user name and you will see the user’s profile.



Search results

Search results when searching for "All users"

Show 50 users per page

□ janesmith □ javentail

2 users found.

Apply user policy template

A user policy template can be applied to the selected users or to all users that are returned in the above search.

Select from templates below

Apply policies

To apply specific policies to the above users, click the button below to view the policies.

Search results

Searching for a group of users: My users

Use this search shortcut to find all users assigned to you.

To search for a group of users (My users):

❶ Click on *AccessAdmin >> Search users >> My users.*

When the search results appear, you can specify the number of results you want to view per page. Select your viewing preference from the Show *drop-down list.*

You can select one or more users by selecting the check box(es) next to the corresponding user.

❷ Set, modify, or view the details for the particular user(s).

Searching for a group of users: MAC-only users

Use this search shortcut to find all users whose authentication method is Mobile ActiveCode (MAC)-only.

This link is only available if you enable MAC-only registration using the IMS Configuration Utility.

To search for a group of users (MAC-only users):

❶ Click on *AccessAdmin >> Search users >> MAC-only users*.

When the search results appear, you can specify the number of results you want to view per page. Select your viewing preference from the Show *drop-down list.*

You can select one or more users by selecting the check box(es) next to the corresponding user.

❷ Set, modify, or just view the details for the particular user(s).

Searching for all Administrators

Using this search shortcut, you can find all Administrators in your IMS Server.

To search for all Administrators:

❶ Click on *AccessAdmin >> Search users >> All administrators*.

When the search results appear, you can specify the number of results you want to view per page. Select your viewing preference from the Show *drop-down list.*

You can select one or more Administrators by selecting the check box(es) next to the corresponding Administrator

❷ Set, modify, or just view the details for the particular Administrator(s).

Searching for all Helpdesk users

Use this search shortcut to find all Helpdesk in your IMS Server.

To search for all Helpdesk users:

❶ Click on *AccessAdmin >> Search users >> All Helpdesks.*

When the search results appear, you can specify the number of results you want to view per page. Select your viewing preference from the Show *drop-down list.*

You can select one or more Helpdesk officers by selecting the check box(es) next to the corresponding Helpdesk.

❷ Set, modify, or just view the details for the particular Helpdesk officer(s).

Searching for all revoked users

Use this search shortcut to find all revoked users in IMS Server.

To search for all revoked users:

❶ Click on *AccessAdmin >> Search users >> All revoked users.*

When the search results appear, you can specify the number of results you want to view per page. Select your viewing preference from the Show *drop-down list.*

You can select one or more revoked users by selecting the check box(es) next to the corresponding revoked user.

❷ Set, modify, or just view the details for the particular revoked user(s).

Viewing and editing user settings

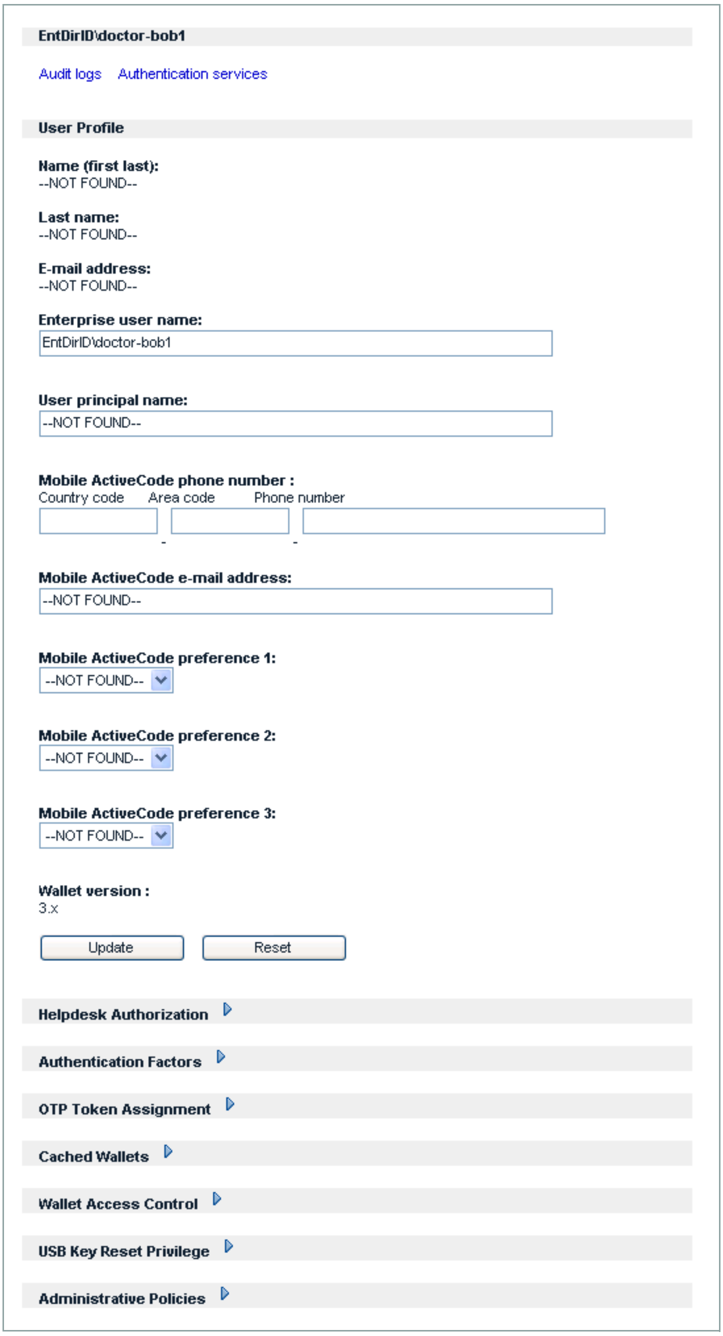
These are some of the user's attributes that you can also view and modify:

- Personal data, including name, email address, Encentuate user name, and other data.
- Mobile ActiveCode preferences (if any)
- Helpdesk authorization panel, for issuance of authorization codes
- Authentication factor(s), their serial number(s) and type(s)
- All cached Wallets and their locations
- The Wallet access control status (available/not available)
- Serial number and other information related to the second authentication factors

- USB Key reset privileges
- Authentication, administrative, password, Wallet, and AccessAgent policies

To view or edit user settings:

1. Search for one user/Helpdesk user/Administrator. For more information, see Searching for users.



EntDirID\doctor-bob1

Audit logs Authentication services

User Profile

Name (first last):
--NOT FOUND--

Last name:
--NOT FOUND--

E-mail address:
--NOT FOUND--

Enterprise user name:
EntDirID\doctor-bob1

User principal name:
--NOT FOUND--

Mobile ActiveCode phone number :
Country code Area code Phone number

Mobile ActiveCode e-mail address:
--NOT FOUND--

Mobile ActiveCode preference 1:
--NOT FOUND--

Mobile ActiveCode preference 2:
--NOT FOUND--

Mobile ActiveCode preference 3:
--NOT FOUND--

Wallet version :
3.x

Viewing user settings

❷ The user’s settings will show the following information:

- The user’s Audit logs

  These are the activity logs for the user which records the time of the activity, the activity, and the result.

- Authentication services

  These are the types of certificate-enabled, enterprise and personal authentication services the user uses, which appears as a link at the top of the page.

For procedures in setting user policies, see Setting user policies.

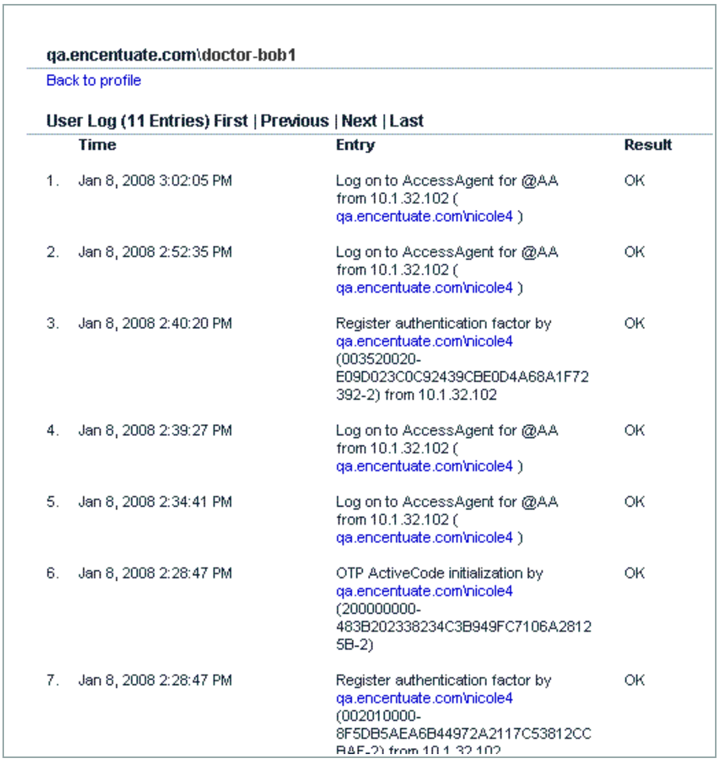
Viewing user audit logs

A Helpdesk officer can only view audit logs. Audit logs contain a detailed list of all user actions.

To view a user audit log:

❶ Search for a user. For more information, see Searching for users.

❷ When you see the user’s settings, click **Audit logs**. The user’s log entries are displayed.



qa.encentuate.com\doctor-bob1

Back to profile

User Log (11 Entries) First | Previous | Next | Last

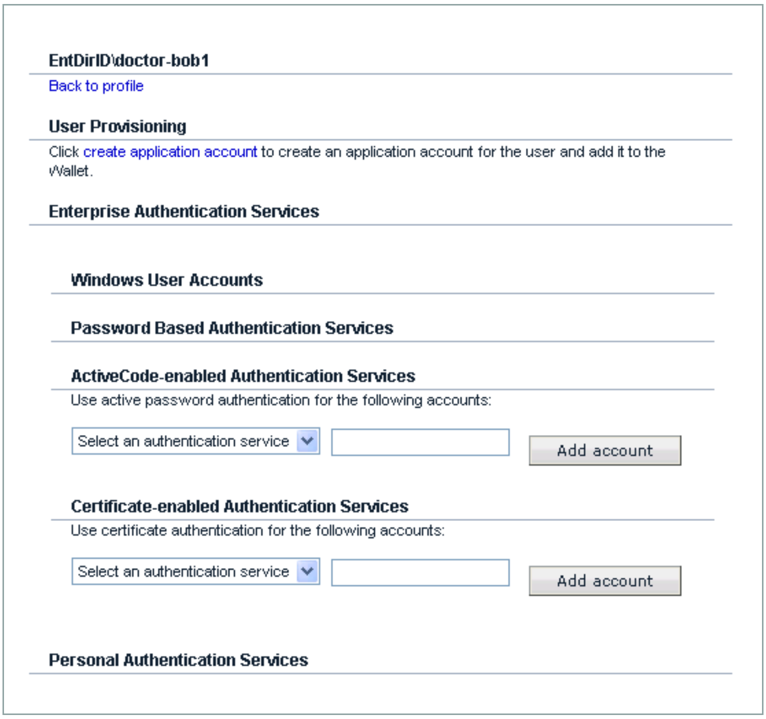
	Time	Entry	Result
1.	Jan 8, 2008 3:02:05 PM	Log on to AccessAgent for @AA from 10.1.32.102 (qa.encentuate.com\nicole4)	OK
2.	Jan 8, 2008 2:52:35 PM	Log on to AccessAgent for @AA from 10.1.32.102 (qa.encentuate.com\nicole4)	OK
3.	Jan 8, 2008 2:40:20 PM	Register authentication factor by qa.encentuate.com\nicole4 (003520020-E09D023C0C92439CBE0D4A68A1F72392-2) from 10.1.32.102	OK
4.	Jan 8, 2008 2:39:27 PM	Log on to AccessAgent for @AA from 10.1.32.102 (qa.encentuate.com\nicole4)	OK
5.	Jan 8, 2008 2:34:41 PM	Log on to AccessAgent for @AA from 10.1.32.102 (qa.encentuate.com\nicole4)	OK
6.	Jan 8, 2008 2:28:47 PM	OTP ActiveCode initialization by qa.encentuate.com\nicole4 (200000000-483B202338234C3B949FC7106A28125B-2)	OK
7.	Jan 8, 2008 2:28:47 PM	Register authentication factor by qa.encentuate.com\nicole4 (002010000-8F5DB5AEA6B44972A2117C53812CCBAF-2) from 10.1.32.102	OK

View a user’s audit logs

Viewing user authentication services

Once users log on to authentication services using Wallet, the information will synchronize with the Encentuate IMS Server via AccessAgent. Encentuate AccessAgent aggregates identities, stores them in the Wallet and synchronizes it with Encentuate IMS Server in real-time.

To view the user's authentication services, search for the user or select one from My Users. Click **Authentication services**.



EntDirID\doctor-bob1

Back to profile

User Provisioning

Click create application account to create an application account for the user and add it to the Wallet.

Enterprise Authentication Services

Windows User Accounts

Password Based Authentication Services

ActiveCode-enabled Authentication Services

Use active password authentication for the following accounts:

Certificate-enabled Authentication Services

Use certificate authentication for the following accounts:

Personal Authentication Services

View user's authentication services

If the organization does not prefer to use Encentuate Wallets with personal authentication services, no entries will be listed under personal authentication services.

Enabling certificates for users

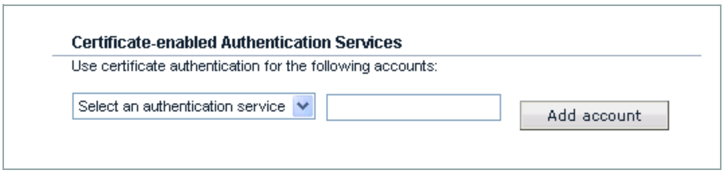
All certificate-enabled authentication services require users to log on with a certificate.

To add a user to a certificate-enabled authentication service:

❶ Search for the user. For more information, see Searching for users.

❷ In the user's settings, click **Authentication services**.

3. Scroll down to **Certificate-enabled authentication services**. From the drop-down list, select the certificate-enabled authentication service you want to add the user to.



Certificate-enabled Authentication Services

Use certificate authentication for the following accounts:

Certificate-enabled authentication services panel

4. Enter the user's name for the certificate-enabled authentication service.

5. Click **Add Account**.

   The certificate-enabled authentication service, including the user name, will be added.

Disabling certificates for users

By disabling certificates for the user, you are temporarily suspending the user's access to the specified certificate-enabled authentication service.

To disable the certificate-enabled authentication service for a user:

1. Search for the user. For more information, see Searching for users.

2. In the user's settings, click **Authentication services**.

3. Scroll down to **Certificate-enabled authentication services**.

4. Mark the check box of the user name and the certificate-enabled authentication services to disable.

5. Select **Disabled** from the Status drop-down list.

6. Click **Update status** to confirm the change.

Deleting certificates for users

You can delete the user's access to a certificate-enabled authentication service when you are certain the user will not use the authentication service again in the future.

Deleting the user's certificate-enabled authentication service account will also revoke all certificates associated with it. Be sure you want to delete the account before you proceed.

To delete a certificate for a user:

❶ Search for the user. For more information, see Searching for users.

❷ In the user's settings, click Authentication services.

❸ Scroll down to Certificate-enabled authentication services.

❹ Mark the check box of the user name to delete for a certificate-enabled authentication service account.

❺ Click Delete account. The delete confirmation window appears.

❻ Click OK to confirm the deletion of the account.

Enabling ActiveCode for the user

When an authentication service is ActiveCode-enabled, users need an ActiveCode whenever they use it.

To add the user to a certificate-enabled authentication service:

❶ Search for the user. For more information, see Searching for users.

❷ In the user's settings, click Authentication services.

❸ Scroll down to ActiveCode-enabled authentication services. From the drop-down list, select the new user's ActiveCode-enabled authentication service.

❹ Enter the user name for the ActiveCode-enabled authentication service.

❺ Click Add Account and the ActiveCode-enabled authentication service, along with the user name, will be added.

Locking ActiveCode for users

To temporarily prevent user from using an ActiveCode-enabled authentication service, you can lock the service. If the user enters the wrong ActiveCode several times in a row, you can also set the service to lock the user automatically.

To lock the ActiveCode-enabled authentication service for a user:

❶ Search for the user. For more information, see Searching for users.

❷ In the user's settings, click Authentication services.

❸ Scroll down to ActiveCode-enabled authentication services.

❹ Mark the check box of the user name and the ActiveCode-enabled authentication service you want to disable.

5. Select **Locked** from the **Status** drop-down list.

6. Click **Update status** to confirm the change.

Deleting ActiveCode for users

You can delete the user's access to an ActiveCode-enabled authentication service if the user will not use the authentication service again in the future.

To delete the ActiveCode-enabled authentication service for a user:

1. Search for the user. For more information, see Searching for users.

2. In the user's settings, click **Authentication services**.

3. Scroll down to **ActiveCode-enabled authentication services**.

4. Mark the check box of the user name you want to delete for a ActiveCode-enabled authentication service account.

5. Click **Delete account**. The delete confirmation window appears.

6. Click **OK** to confirm the deletion of the account.

Generating authorization codes for users

Users need authorization codes if:

- they lost their second authentication factor(s)

- they forgot their Encentuate password

To create an authorization code for a user:

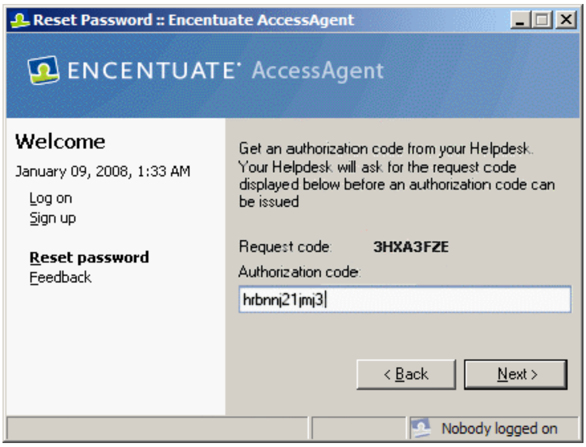
1. Search for the user. For more information, see Searching for users.

2. Ask the user whether a request code is displayed onscreen.

    - If there is a request code, click **Temporary offline access to the Wallet** in the Helpdesk Authorization panel, and enter the authorization request code.

      The user has a request code because connectivity to the IMS Server may not be available. As a security measure, the user must provide a request code before you can issue an authorization code for temporary offline access.

You must inform the user that for temporary offline access, the new password is only valid for that computer.



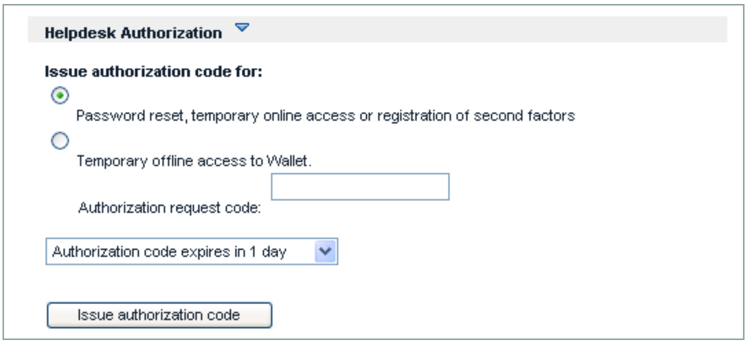
January 09, 2008, 1:33 AM

Get an authorization code from your Helpdesk. Your Helpdesk will ask for the request code displayed below before an authorization code can be issued

Request code: 3HXA3FZE

Authorization code: hrbnnj21jmj3

User's AccessAgent window - Request code



● Password reset, temporary online access or registration of second factors

○ Temporary offline access to Wallet.

Authorization request code:

Authorization code expires in 1 day

Temporary offline access

- If there is NO request code, click **Password reset, temporary online access or registration of second factors** in the Helpdesk Authorization panel.

3. Enter the **Request Code** as dictated by the user. This code is *not* case-sensitive.

4. Select a validity period from the options available in the drop-down list.

5. Click **Issue authorization code.**

An authorization code appears and can now be relayed to the user. The authorization code is a random alphanumeric code used for retrieving credentials. The code is *not* case-sensitive, thus omit the hyphens and uppercase characters. Each new authorization code replaces the previously issued one. The authorization code should be used as soon as possible.

Once the user uses the authorization code to register a new second authentication factor, its information synchronizes with the IMS Server and will be displayed under the user's settings.

Viewing and revoking authentication factors

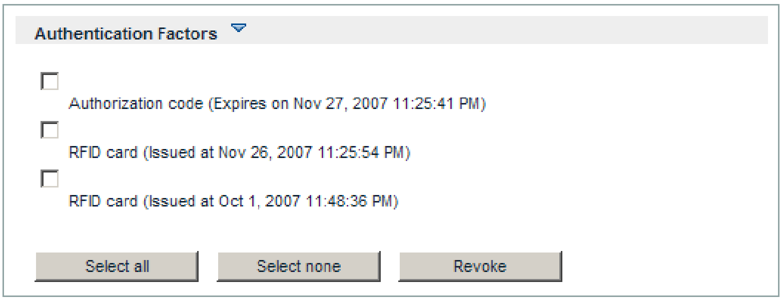
When users sign up for a new Encentuate Wallet or registers a second authentication factor, this information is synchronized with the IMS Server. An entry with the corresponding second authentication factor is added under the user's settings. This allows you to view the user's various types of second authentication factors.

You can revoke a second authentication factor or Wallet when the user leaves the company or when a second authentication factor is reported lost or stolen.

To revoke a Wallet or an authentication factor:

❶ Search for the user. For more information, see Searching for users.

❷ In the user's settings, scroll down to the Authentication Factors panel. All authentication factors are displayed. Mark the check box of the Wallet or authentication factor to revoke.



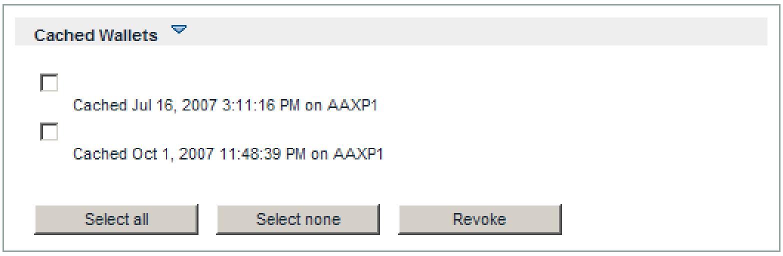
□ Authorization code (Expires on Nov 27, 2007 11:25:41 PM)
□ RFID card (Issued at Nov 26, 2007 11:25:54 PM)
□ RFID card (Issued at Oct 1, 2007 11:48:36 PM)

Registered authentication factors

❸ Click Revoke.

Viewing and revoking cached Wallets

When the user saves the Wallet in a computer's cache, the information is synchronized with the IMS Server. An entry with the corresponding computer's name is added under the user's settings. This allows you to view the computers assigned to the user.



□ Cached Jul 16, 2007 3:11:16 PM on AAXP1
□ Cached Oct 1, 2007 11:48:39 PM on AAXP1

Cached wallets

You can revoke a cached Wallet when the user leaves the organization or when a second authentication factor is reported lost or stolen.

Ideally, you can revoke or delete a user and the assigned authentication factor when the user leaves the organization. Delete the cached Wallets if the machine contains too many Wallets that are no longer needed.

To revoke a cached Wallet:

1. Search for the user. For more information, see Searching for users.
2. In the user's settings, scroll down to the Cached Wallet panel. All cached Wallets are displayed. Mark the check box of the Wallet to revoke.
3. Click **Revoke**.

Locking and unlocking Wallets

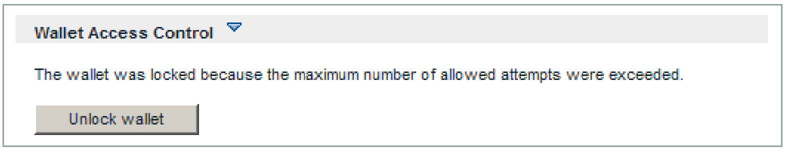
When the user logs on with the wrong password and exceeds the maximum number of allowed attempts, the system will lock the Wallet. When this happens, the user must contact Helpdesk or the Administrator to unlock the Wallet.

You can also lock a Wallet for other possible reasons, such as:

- To temporarily bar access to the user's Wallet (for example, when the user goes for an extended holiday).
- When an employee leaves the organization, the Wallet can be locked until the user is de-provisioned or revoked from the IMS Server.

To lock/unlock a Wallet:

1. Search for the user. For more information, see Searching for users.



The wallet was locked because the maximum number of allowed attempts were exceeded.

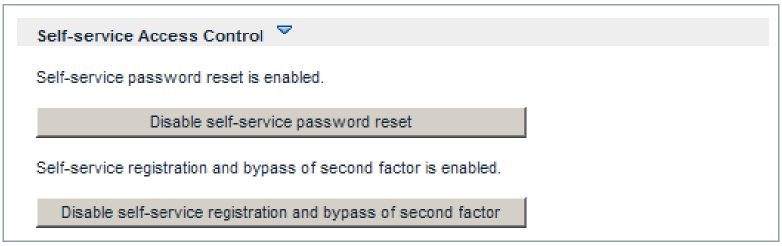
Locking or unlocking the Wallet

2. Click **Lock/Unlock**.

Enabling self-service access

AccessAssistant and Web Workplace offer a host of self-service capabilities to users. Without AccessAgent, users must know the application passwords to log on to enterprise applications. AccessAssistant allows users to view their application passwords or copy them to the clipboard.

Users can also reset their secret questions and answers through AccessAssistant or Web Workplace. Instead of calling Helpdesk for an authorization code, the self-service feature allows users to reset their Encentuate passwords after providing a subset of previously specified secrets.



Self-service Access Control

Self-service password reset is enabled.

Disable self-service password reset

Self-service registration and bypass of second factor is enabled.

Disable self-service registration and bypass of second factor

Self-service password reset

Aside from using self-service access, users can also reset passwords through AccessAgent:

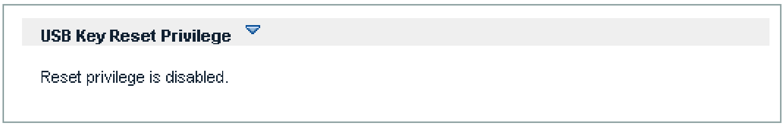
- Click **Reset password** from AccessAgent.

  AccessAgent prompts the user to select secret questions (previously specified) and provide the corresponding answers.

- Specify a new Encentuate password. After resetting successfully, the user can log on using the new Encentuate password.

Viewing statuses of USB Key reset privileges

Encentuate USB Keys can only be reset by Administrators with reset privileges, which is granted from the USB Key Utility. This panel provides information on whether or not an Administrator has reset privileges.



USB Key Reset Privilege

Reset privilege is disabled.

Reset privilege

For more information on using the USB Key Utility, or granting reset privilege, see the *Encentuate USB Key Utility Guide*.

Setting Policies

All policies with system, machine, or user scope can be modified through AccessAdmin. User policies can also be modified for an entire group of users by using the **Search Users** feature. System policies may be defined for authentication services, applications, or a combination of authentication service and application. This section discusses how to view and set system, user, and machine policies using Encentuate AccessAdmin.

- General procedure for setting a policy
- Setting user policies
- Setting system policies
- Setting policy priorities

General procedure for setting a policy

To set a policy, it is necessary to determine its scope as well as whether there are dependencies on other policies. This information is available Definitions of policies.

The general procedure for setting a policy is as follows:

Look for the policy in Definitions of policies.

Read the notes carefully to determine if there are dependencies on other policies or configuration settings. If there are, ensure that the dependent policies and configuration settings are set appropriately.

Identify the available scopes (in the **Scope** column) of the policy. If there are multiple scopes, choose the desired scope and set the corresponding policy priority (a system policy, which is listed in the notes) appropriately.

If the scope is User, and you want to modify the policy for a user, log on to AccessAgent as Administrator or Helpdesk, launch AccessAdmin, search for the user, and look for the setting that matches the policy's **IMS Entry** column.

If the scope is User, and you want to modify the policy in a policy template, you must log on to AccessAgent as Administrator, launch AccessAdmin, navigate to the desired policy template, and look for the setting that matches the policy's **IMS Entry** column.

If the scope is System, you must log on to AccessAgent as Administrator, launch AccessAdmin, navigate to System Policies (or Authentication Service Policies/ Application Policies, if it is applied to a particular authentication service or application), and look for the setting that matches the policy's **IMS Entry** column.

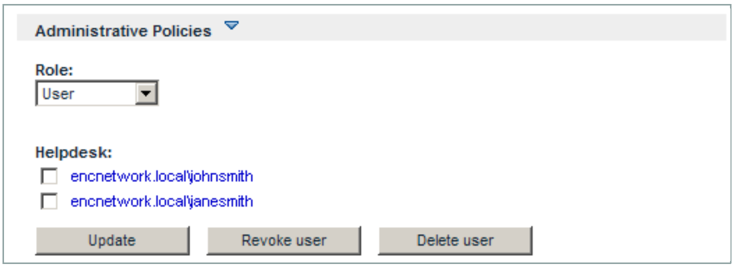
If the scope is Machine, and you want to modify the policy for a particular machine, go to *AccessAdmin >> Machine Policy Templates*. For more information, see Applying policy templates to machines.

The new policy value may only be applicable immediately, after the next synchronization between AccessAgent and IMS Server, or after the machine is restarted. Check the **refreshed on ....** specification in the policy's **Values** column.

Setting user policies

Setting administrative policies

There are three roles within Encentuate IAM: user, Helpdesk, and Administrator. An Administrator has the right to promote the user or a Helpdesk, as well as to demote a Helpdesk. However, an Administrator cannot demote himself.



Administrative Policies

Role: User

Helpdesk:

□ encnetwork.local\johnsmith

□ encnetwork.local\janesmith

Role modification

You can also revoke and delete the user that no longer needs to use Encentuate IAM or any of its components.

The profile and logs of a revoked user are stored in the IMS Server even though the Encentuate Wallet or authentication factors can no longer be used. However, when you delete a user, all user data will be purged from the server, including audit logs. Before deleting a user from the database, make sure that this user will no longer be needed for any purpose.

To modify roles:

1. Search for the user. For more information, see Searching for users.

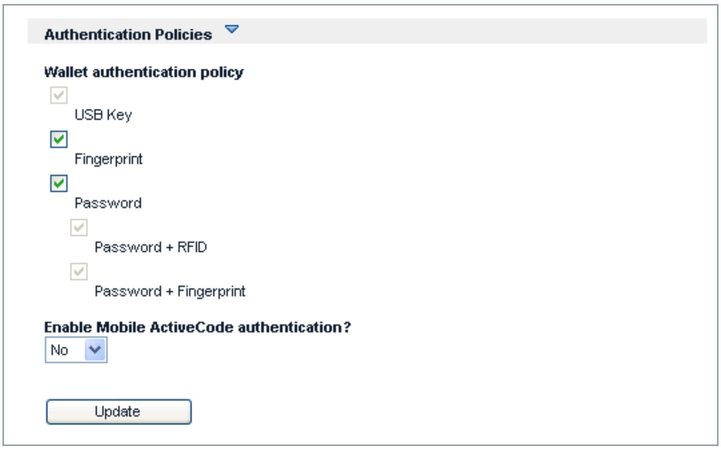
2. In the user's settings, scroll down to the Administrative Policies panel. All the users and Helpdesk personnel assigned to you are displayed. Select the check box corresponding to the user you want to promote.

3. Click **Update**.

   To revoke the user, click **Revoke user**. To delete the user, click **Delete user**.

Setting authentication policies

In this panel, set Wallet authentication policies for individual users to enforce the combinations of authentication factors that can be used to log on.



Authentication Policies

Wallet authentication policy

☑ USB Key

☑ Fingerprint

☑ Password

☑ Password + RFID

☑ Password + Fingerprint

Enable Mobile ActiveCode authentication?

No

Authentication policies

When setting your Wallet authentication policy, take note of the following:

- If you select **USB Key**, it is automatically assumed that a USB Key password is required.
- If **Fingerprint** is selected, fingerprint authentication is required.
- If the **Password** option is selected, the two sub-policies are enabled. You can then modify the sub-policies as required. **RFID** also includes the Active Proximity Badge.

Mark the corresponding check box(es) to select a Wallet authentication policy.

In this panel, you can also:

- **Enable Mobile ActiveCode authentication**

  If this policy is enabled, the user can authenticate using Encentuate Mobile ActiveCode. Select **Yes** or **No**.

To confirm the changes, click **Update**.

Setting Encentuate password policies

You can set the following password policies for the user:

- **Set the Encentuate password to the last-changed USB Key password**

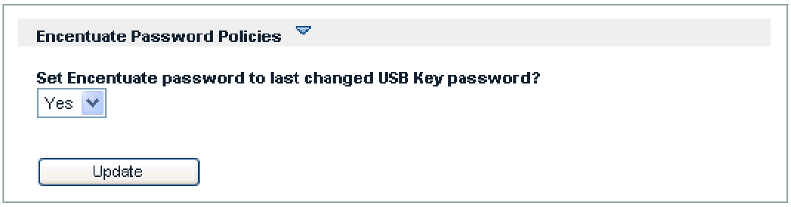
  The Encentuate password is different from the USB Key password. The USB Key's smart card is protected by its own password, which needs to be periodically synchronized with the Encentuate password.

  For users who typically only has one USB Key, this policy should be enabled.

  For power users who may have more than one USB Keys, this policy should be disabled.

- **Force pre-provisioned user to change the Encentuate password at first logon**

  In some deployment scenarios, users are pre-provisioned by a Helpdesk officer or an Administrator—this means that the Encentuate password is known to people other than the user. Enable this policy to make sure the user changes the Encentuate password upon first logon.



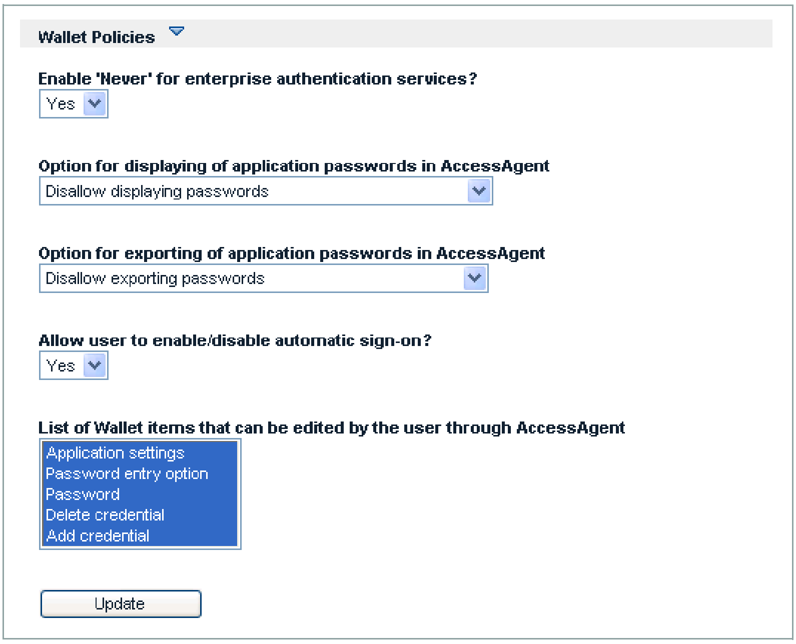
Encentuate Password Policies

Set Encentuate password to last changed USB Key password? Yes

Password policies

Use the drop-down lists to modify the policies. To confirm the changes, click **Update**.

Setting Wallet policies



Wallet Policies

Enable 'Never' for enterprise authentication services?
Yes

Option for displaying of application passwords in AccessAgent
Disallow displaying passwords

Option for exporting of application passwords in AccessAgent
Disallow exporting passwords

Allow user to enable/disable automatic sign-on?
Yes

List of Wallet items that can be edited by the user through AccessAgent
Application settings
Password entry option
Password
Delete credential
Add credential

Wallet policies

You can set Wallet policies for the user, which regulate the following Wallet behaviors:

- Enable "Never" for enterprise authentication services

  If enabled, the user can set an enterprise authentication services' password entry option to **Never**.

  If disabled, the password entry option will not have the option **Never**.

- Supported authentication modes

  This policy specifies the authentication mode(s) that can be employed to access a Wallet.

Use the drop-down lists to modify the policies, or hold down the **Shift** key or **Ctrl** key on your keyboard while clicking to select more than one supported authentication modes.

✓ *Encentuate recommends using the system default.*

To confirm the changes, click **Update**.

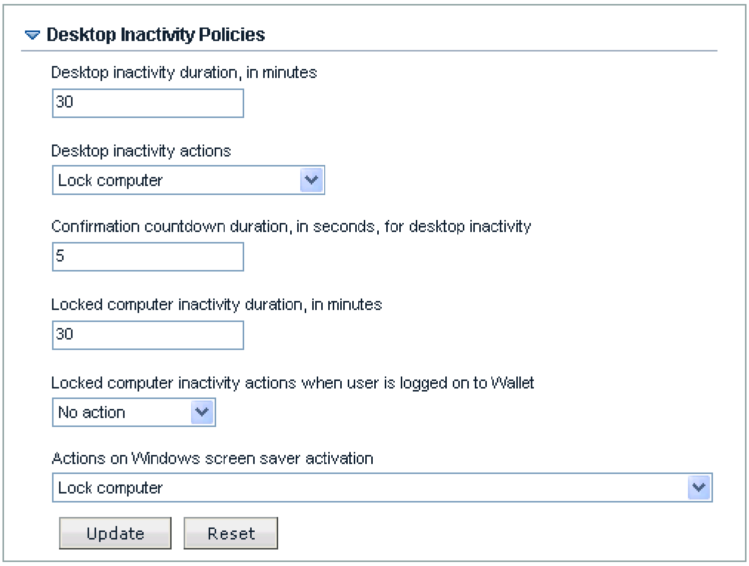
Setting AccessAgent policies

AccessAgent policies consists of all the policies that define the behavioral patterns of AccessAgent on one computer when the user is logged on. The AccessAgent policies cover the following behavioral patterns:

Desktop inactivity policies

- Desktop inactivity duration, in minutes

  Desktop inactivity duration, in minutes, after which AccessAgent may perform a set of actions.



Desktop Inactivity Policies

Desktop inactivity duration, in minutes: 30

Desktop inactivity actions: Lock computer

Confirmation countdown duration, in seconds, for desktop inactivity: 5

Locked computer inactivity duration, in minutes: 30

Locked computer inactivity actions when user is logged on to Wallet: No action

Actions on Windows screen saver activation: Lock computer

Desktop inactivity policies

- Desktop inactivity actions

  Actions to be performed by AccessAgent after a period of desktop inactivity.

- Confirmation countdown duration, in seconds, for desktop inactivity

  Before AccessAgent takes the specified action for desktop inactivity, a message box will appear to inform the user that AccessAgent will take action due to desktop inactivity.

  The user can either click Yes to let AccessAgent take the action, or No to re-activate the desktop. If the user clicks neither during the specified countdown time frame, AccessAgent takes the action specified for desktop inactivity.

- Locked computer inactivity duration, in minutes

  The time frame for desktop inactivity, after which AccessAgent take an action (for example lock the computer).

- Locked computer inactivity actions when user is logged on to the Wallet

  The action that AccessAgent takes when desktop inactivity time has exceeded the specified limit.

- Actions on Windows screen saver activation

  If Windows screen saver is used for the computer, desktop inactivity duration follows the Windows countdown. Here, you can specify the action that AccessAgent will take upon Windows screen saver activation.

Use the drop-down lists to modify the policies, or enter the values.

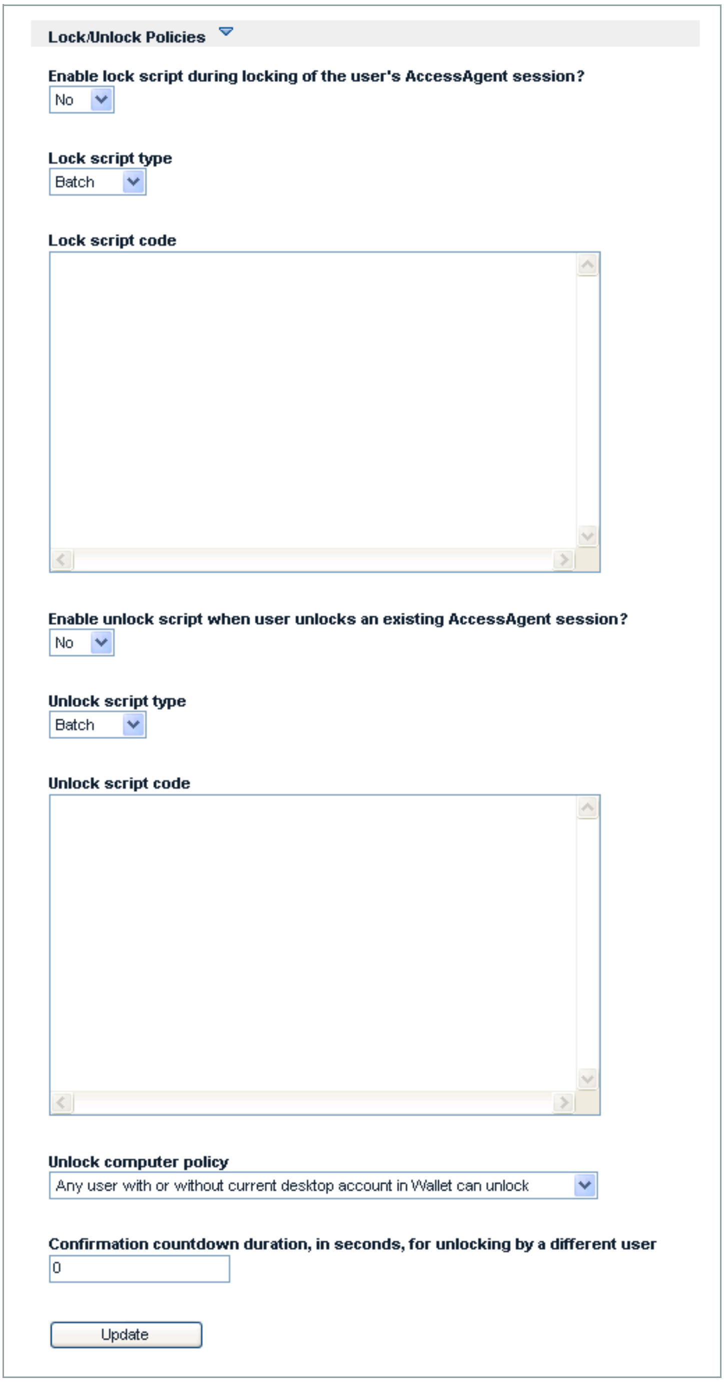
To confirm the changes, click Update.

Lock/unlock policies

Lock or unlock scripts can be written to perform actions right before the user locks or right after the user unlocks the screen.

The lock and unlock scripts should be included in the policy template.

To confirm the changes, click Update.



Lock/Unlock Policies

Enable lock script during locking of the user's AccessAgent session?
No

Lock script type
Batch

Lock script code

Enable unlock script when user unlocks an existing AccessAgent session?
No

Unlock script type
Batch

Unlock script code

Unlock computer policy
Any user with or without current desktop account in Wallet can unlock

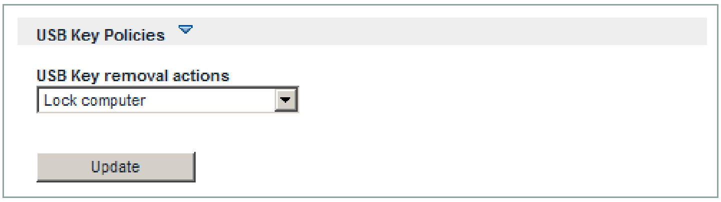
Confirmation countdown duration, in seconds, for unlocking by a different user
0

Lock and unlock policies

Second authentication factor-related policies

These are the second authentication factor-specific policies, which means they do not apply if the user does not use the second authentication factor that the policy was specified for.

USB Key policies


USB Key Policies

USB Key removal actions

Lock computer

USB Key Policies

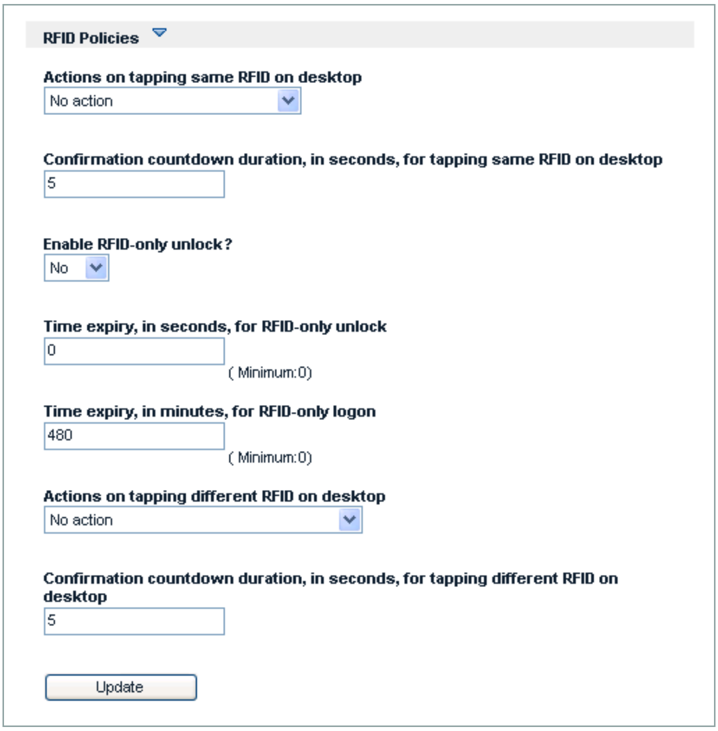
- USB Key removal actions

  This policy specifies the action that AccessAgent will take upon the removal of the USB Key from the port.

Use the drop-down lists to modify the policies.

To confirm the changes, click **Update**.

RFID policies


RFID Policies

Actions on tapping same RFID on desktop

No action

Confirmation countdown duration, in seconds, for tapping same RFID on desktop

5

Enable RFID-only unlock?

No

Time expiry, in seconds, for RFID-only unlock

0

(Minimum:0)

Time expiry, in minutes, for RFID-only logon

480

(Minimum:0)

Actions on tapping different RFID on desktop

No action

Confirmation countdown duration, in seconds, for tapping different RFID on desktop

5

RFID policies

- Actions on tapping same RFID on desktop

  The action that AccessAgent takes when the logged on user taps the RFID Card on the reader once again.

- Confirmation countdown duration, in seconds, for tapping same RFID on desktop

  This policy specifies the countdown time frame for the specified action to take place after tapping the same RFID Card on the reader. A message box appears, with a countdown timer asking the user if AccessAgent should take the action specified for same RFID tap.

  The user can either click Yes to let AccessAgent take the action, or No to re-activate the desktop. If the user clicks neither during the specified countdown time frame, AccessAgent takes the action specified for same RFID tap.

- Actions on tapping different RFID on desktop

  The action that AccessAgent takes when another user taps the RFID Card on the reader, even though there is one user already logged on.

- Confirmation countdown duration, in seconds, for tapping different RFID on desktop

  This policy specifies the countdown time frame for the specified action to take place after tapping a different RFID Card on the reader. A message box appears, with a countdown timer asking the user if AccessAgent should take the action specified for different RFID tap.

  The user can either click Yes to let AccessAgent take the action, or No to re-activate the desktop. If the user clicks neither during the specified countdown time frame, AccessAgent takes the action specified for different RFID tap.

Use the drop-down lists to modify the policies, or enter the values.

To confirm the changes, click Update.

Fingerprint Identification policies

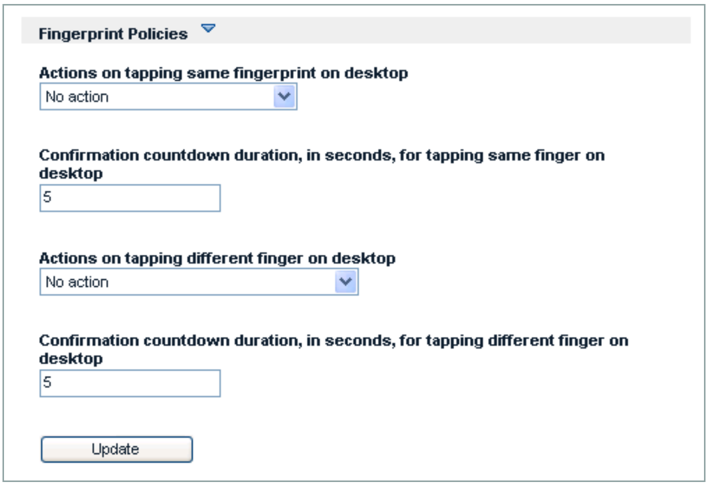
- Actions on imprinting same finger on desktop

  The action that AccessAgent takes when a logged on user imprints finger on the fingerprint reader.

- Confirmation countdown duration, in seconds, for imprinting same finger on desktop

  This policy specifies the countdown time frame for the specified action to take place after a logged on user imprints finger on the fingerprint reader. A message box appears, with a countdown timer asking the user if AccessAgent should take the action specified for the finger imprint.

  The user can either click Yes to let AccessAgent take the action, or No to re-activate the desktop. If the user clicks neither during the specified countdown time frame, AccessAgent takes the action specified for the finger imprint.



Fingerprint Policies

Actions on tapping same fingerprint on desktop

No action

Confirmation countdown duration, in seconds, for tapping same finger on desktop

5

Actions on tapping different finger on desktop

No action

Confirmation countdown duration, in seconds, for tapping different finger on desktop

5

Fingerprint policies

- **Actions on imprinting different finger on desktop**

  The action that AccessAgent takes when another user imprints finger on the reader, even though there is one user already logged on.

- **Confirmation countdown duration, in seconds, for imprinting different finger on desktop**

  This policy specifies the countdown time frame for the specified action to take place after imprinting a different finger on the fingerprint reader. A message box appears, with a countdown timer asking the user if AccessAgent should take the action specified for different finger imprint.

  The user can either click **Yes** to let AccessAgent take the action, or **No** to re-activate the desktop. If the user clicks neither during the specified countdown time frame, AccessAgent takes the action specified for different finger imprint.

Use the drop-down lists to modify the policies, or enter the values.

To confirm the changes, click **Update**.

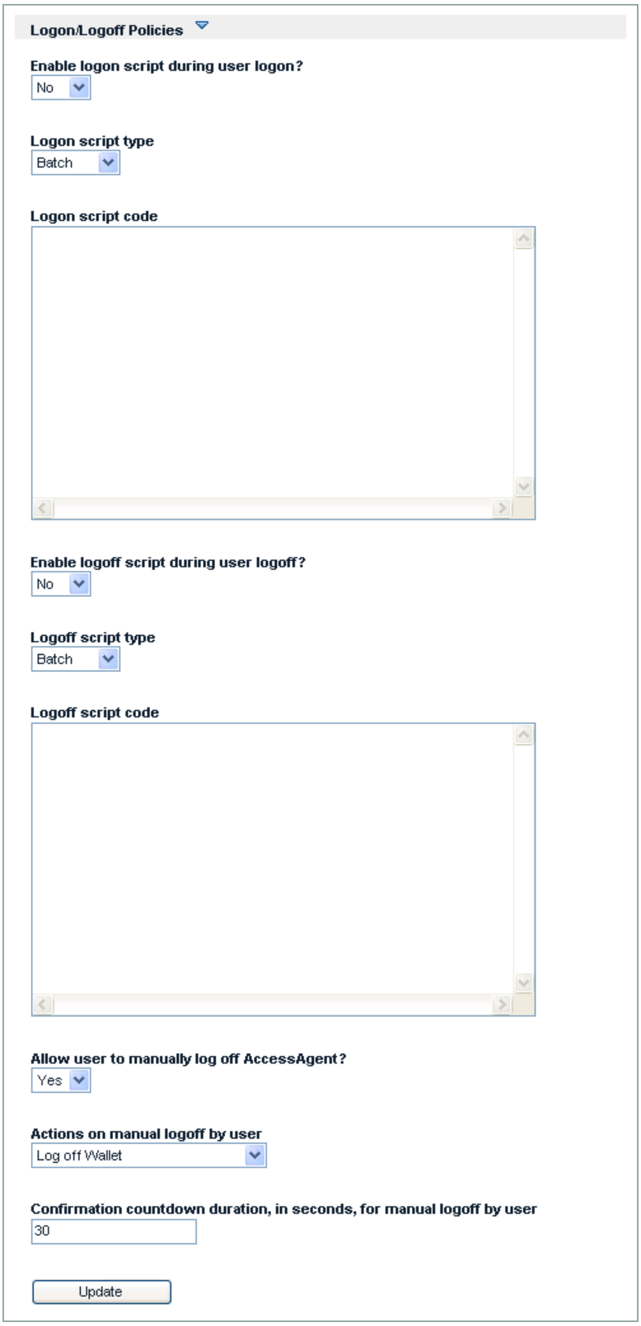
Logon/logoff policies

The logon/logoff policies define the behavioral patterns of AccessAgent when the user logs on to or logs off AccessAgent.

- **Enable logon script during user logon**

  If this policy is enabled, a script will run whenever the user logs on to AccessAgent. The script specifies various actions that AccessAgent will take upon

  logon, such as which applications to start, which network resources to reconnect to, etc.



Logon/Logoff Policies

Enable logon script during user logon?
No

Logon script type
Batch

Logon script code

Enable logoff script during user logoff?
No

Logoff script type
Batch

Logoff script code

Allow user to manually log off AccessAgent?
Yes

Actions on manual logoff by user
Log off Wallet

Confirmation countdown duration, in seconds, for manual logoff by user
30

Logon and logoff policies

- **Logon script type**

  These are the types of logon script you can use with AccessAgent. You can either select Batch file or VB script.

- **Logon script code**

  You can copy the logon script and paste it here.

- Enable logoff script during user logoff

  Enabling this policy means a script will run whenever the user logs off AccessAgent. The logoff script dictates the actions that take place upon logoff, such as which applications to close, which network resources to disconnect from, etc.

- Logoff script type

  These are the types of logoff script you can use with AccessAgent. You can either select Batch file or VB script.

- Logoff script code

  You can copy the logoff script and paste it here.

- Actions on logoff

  The action AccessAgent takes when the user logs off.

- Confirmation countdown duration, in seconds, for logoff

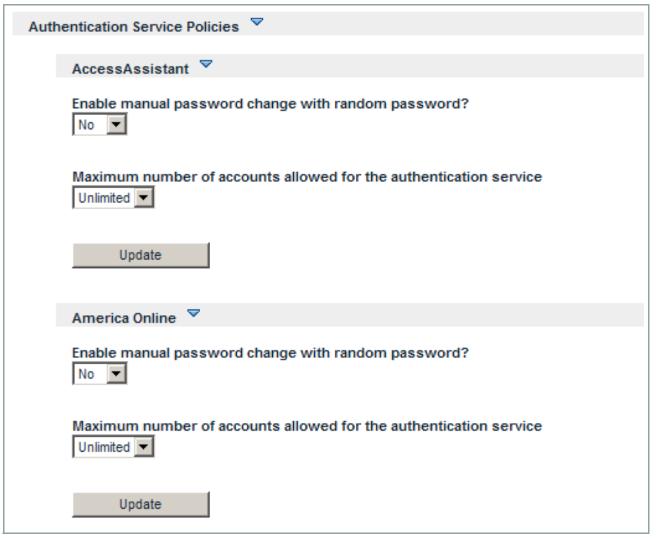
  This policy specifies the time it takes the computer to confirm logoff, after the system has been idle for a while.

Use the drop-down lists to modify the policies, or enter the values.

To confirm the changes, click **Update**.

Setting authentication service policies

Authentication service policies apply to each enterprise authentication service.



Authentication Service Policies

AccessAssistant

Enable manual password change with random password? No

Maximum number of accounts allowed for the authentication service Unlimited

America Online

Enable manual password change with random password? No

Maximum number of accounts allowed for the authentication service Unlimited

Authentication service policies

For every authentication service, you can specify:

- Enabling manual password change with random password

  If this policy is enabled, when the user changes password manually, AccessAgent auto-fills a randomly generated new password for the user.

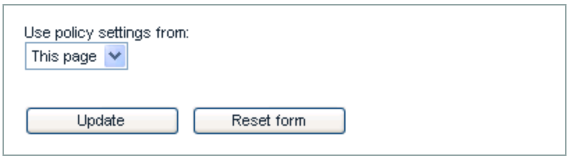
Use the drop-down lists to modify the policies.

To confirm the changes, click **Update**.

Applying policies defined on the page

When you have finished making changes to the policy settings, click **Update** at the bottom of the user profile page.

To cancel changes, click **Reset form**.



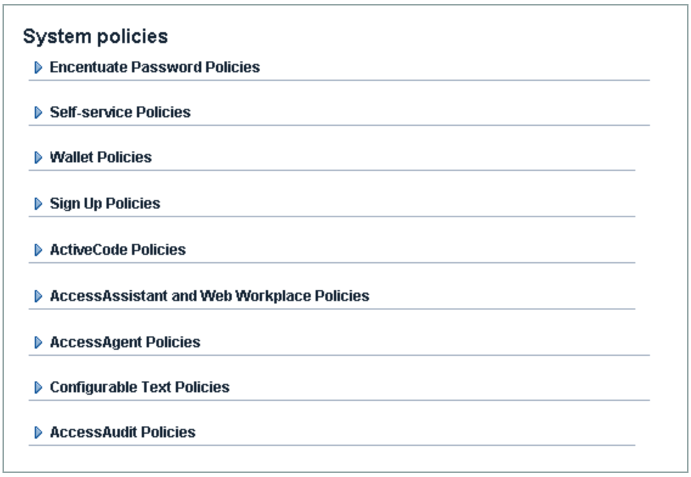
Use policy settings from: This page

Click Reset form

Setting system policies

To set system policies:

1. In the AccessAdmin navigation panel, select *System >> System policies*.



System policies screen

❷ You can view the details of each policy and modify them by expanding the panels using the down arrow ▼. You can also hide the details using the right arrow ▷.

Custom events tracking

You create custom events to track application-specific events such as:

- Access to confidential data
- Attempted access to application features for which user is not authorized to use
- Access to application outside office hours

Custom events are created as a list of event code and display text pairs.

To create custom events:

❶ Go to *System Policies >> AccessAudit Policies*.

❷ Add each pair of event code and display text to “List of custom audit event codes and their corresponding display names”. Each event is entered as “<Event Code>,<Display Text>” where event code is a hexadecimal code in the range 0x43015000 to 0x43015FFF, inclusive. For example, “0x43015001,Access to confidential data”.

❸ Using AccessStudio, create an AccessProfile that tracks the event and submits an audit log with that event code.

Setting policy priorities

If a policy is defined for two scopes (e.g: machine and system; user and system; machine and user), we need to define a priority in case the time-out value is different for one scope and the other.

For example, if the policy priority is “machine”, then only the machine policy would be effective.

Policies can be modified only by Helpdesk officers and Administrators, because these policies affect the behavior of the whole system and should only be modified when it is absolutely necessary.

These policies should be set at deployment and followed through. Changes to these policies are propagated to clients the next time AccessAgent synchronizes with the IMS Server.

Use the **managepolicy.bat** Command Line Tool (CLT) to view and modify policy priorities. This CLT allows Administrators to retrieve the priority of a given policy, as well as set its priority by identifying a valid policy ID and scope.

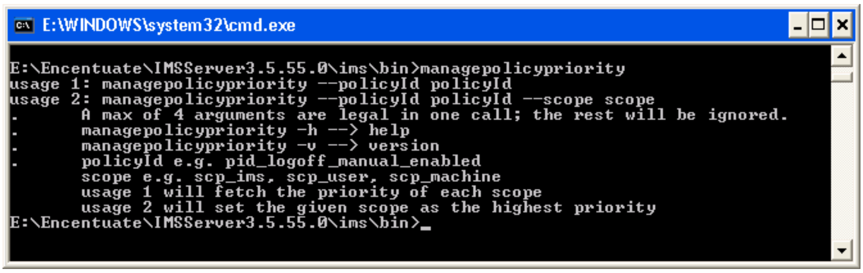
Older versions of AccessAgent will still use the original policy priorities, and values will not change after IMS is upgraded. To change policy priorities, upgrade all installations of AccessAgent 3.6 and above, and then run the CLT.

To view the current priority of a policy:

1. Click *Start* >> *Run* from your Windows Desktop. Enter **cmd** to launch the Command Line Tool.

2. Navigate to the folder of the batch file by entering **cd\Encentuate\[IMS Server folder]\ims\bin**, then press **Enter**.

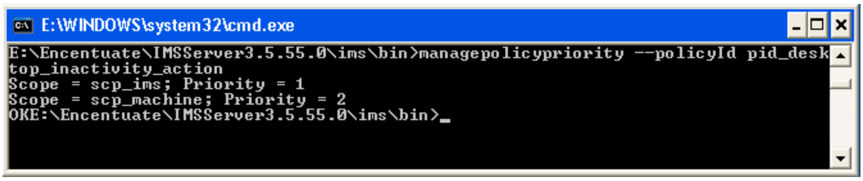
3. Enter **managepolicypriority** to view the information on executing the batch file, then press **Enter**. The details are displayed on the window.



```
E:\Encentuate\IMSServer3.5.55.0\ims\bin>managepolicypriority
usage 1: managepolicypriority --policyId policyId
usage 2: managepolicypriority --policyId policyId --scope scope
.       A max of 4 arguments are legal in one call; the rest will be ignored.
.       managepolicypriority -h --> help
.       managepolicypriority -v --> version
.       policyId e.g. pid_logoff_manual_enabled
        scope e.g. scp_ims, scp_user, scp_machine
        usage 1 will fetch the priority of each scope
        usage 2 will set the given scope as the highest priority
E:\Encentuate\IMSServer3.5.55.0\ims\bin>_
```

Executing the batch file

4. To view the scope and priority of a specific policy, enter **managepolicypriority --policyId [name of policy]**, then press **Enter**. The scope and priority of a policy is displayed.



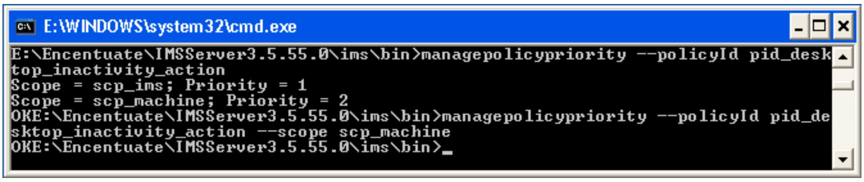
```
E:\Encentuate\IMSServer3.5.55.0\ims\bin>managepolicypriority --policyId pid_desk
top_inactivity_action
Scope = scp_ims; Priority = 1
Scope = scp_machine; Priority = 2
OKE:\Encentuate\IMSServer3.5.55.0\ims\bin>_
```

Policy scope and priority

To set the priority of a policy:

1. Get the path from the folder of the batch file (**cd\Encentuate\[IMS Server folder]\ims\bin**), then press **Enter**.

2. To change the scope of the policy, enter **managepolicypriority --policyId [name of policy] --scope [scp_ims or scp_machine]**, then press **Enter**.



```
E:\Encentuate\IMSServer3.5.55.0\ims\bin>managepolicypriority --policyId pid_desk
top_inactivity_action
Scope = scp_ims; Priority = 1
Scope = scp_machine; Priority = 2
OKE:\Encentuate\IMSServer3.5.55.0\ims\bin>managepolicypriority --policyId pid_de
sktop_inactivity_action --scope scp_machine
OKE:\Encentuate\IMSServer3.5.55.0\ims\bin>_
```

Changing the policy scope

The scope that will be given first priority is assigned a value of "1", the next scope a value of "2", and so on.

❸ Enter **exit** to close the command prompt.

Managing Policy Templates

This chapter discusses how to use policy templates in Encentuate AccessAdmin. There are two ways to log on to AccessAdmin:

- Go to the console of the machine where the IMS Server is installed, access https://imsservername, and a logon prompt will be presented; or
- Log on to AccessAgent on any machine as Administrator, and then launch https://imsservername.

When logging on to AccessAdmin, enter the fully qualified domain name (for example, https://ims.encentuate.com).

If the IMS server is accessed without using the fully qualified domain name, AccessAgent cannot perform logon to search page automatically.

In the main user interface, you can find links to all the available administration functions. The main link, AccessAdmin, should be visible at all times. Click the link to view the AccessAdmin user interface.

This chapter covers the following topics:

About policy templates

A policy template is a set of pre-defined user or machine policies which can be applied to IMS users or machines.

Encentuate AccessAdmin supports dynamic non-hierarchical groups, collapsible sections, and the setting of policies for groups and users. Attributes that define logical groups (for example, department) can be obtained directly from the corporate directory. When the user signs up or a machine joins the IMS Server, policies are initially assigned based on the machine's/user's attributes that match the policy template.

Subsequently, user groups are dynamic because membership depends on the user's policies. For example, a user may belong to the RFID user group if assigned with a "Password + RFID" authentication policy. By changing the authentication policy for the user to "USB Key", the user becomes a member of the USB Key users group.

User policy modifications may be performed on individual users or on entire groups of users. The user may belong to the group of all USB Key users as well as the group of all AccessAssistant users. Groups, being based on search criteria, are virtual and overlapping.

User policy templates can be defined for specific groups of users to facilitate policy setting. For example, a template can be defined for the Finance department. Any new user whose department attribute is "Finance" will have policies initialized with the template settings.

Machine policy templates are defined for each machine that joins the IMS Server. These policies are under scope:machine (scp_machine), and keyed on the machine name. The machine policies are synced through incremental synchronization based on the machine name.

Machines can be assigned to an existing machine policy template based on either or all of the following attributes:

- Machine name
- IP address
- AccessAgent version
- OU group
- Active Directory security group

All policies with system, machine or user scope can be modified through AccessAdmin. User policies can also be modified for an entire group of users by using the "Search Users" feature. System policies may be defined for authentication services, applications, or a combination of authentication service and application.

The Helpdesk role can be defined for different groups of users. The user taking on the Helpdesk role associated with a group is able to manage (for example, authorize and revoke) users only for that group. Helpdesk officers may manage overlapping groups of users.

As an Administrator, you can view, modify, create, and delete policy templates.

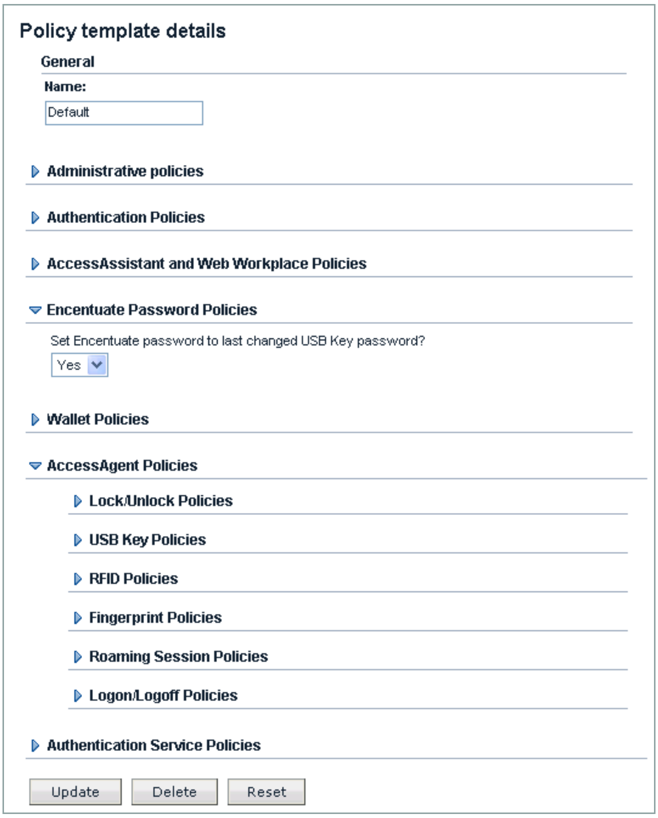
Viewing a template

To view a template:

❶ In the AccessAdmin navigation panel, select *User Policy Templates or Machine Policy Templates >> [name of template].*

There is one Default template in case the Administrator has defined other templates under the Policy Templates option in the navigation panel. The other templates are fully configurable, so the naming convention depends on your enterprise's corporate rules.

❷ You can view the details of each policy by expanding the panels using the down arrow ▼ . You can also hide the details using the right arrow ▷ .



Policy template details

General

Name: Default

▷ Administrative policies

▷ Authentication Policies

▷ AccessAssistant and Web Workplace Policies

▼ Encentuate Password Policies

Set Encentuate password to last changed USB Key password? Yes

▷ Wallet Policies

▼ AccessAgent Policies

▷ Lock/Unlock Policies

▷ USB Key Policies

▷ RFID Policies

▷ Fingerprint Policies

▷ Roaming Session Policies

▷ Logon/Logoff Policies

▷ Authentication Service Policies

Modifying a policy template

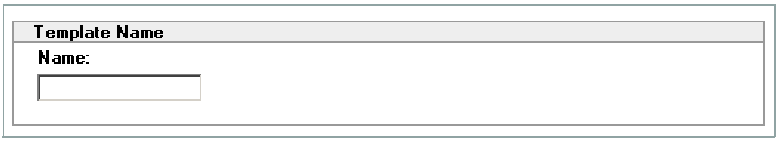
Creating a new template

You can create a new policy template using AccessAdmin. A customized template allows you to apply a set of policies to a specific set of users or machines that you manage.

To create a new user policy template:

❶ Click *AccessAdmin >> User Policy Templates >> New template*.

❷ Enter a Template Name.



Template Name

Name:

Enter template name

❸ In the Administrative Policies panel, select the Helpdesk officer(s) to whom this new policy will apply, by selecting the corresponding check box(es). You can modify your selection later.

❹ Show the policies by clicking the arrow in the panel heading to expand it. You can modify any of these policies.

❺ When you have finished making your selections, click Update. The new template will appear in the AccessAdmin navigation panel on the left side of the browser.

If you have changed your mind and no longer want to create a new template, click Reset.

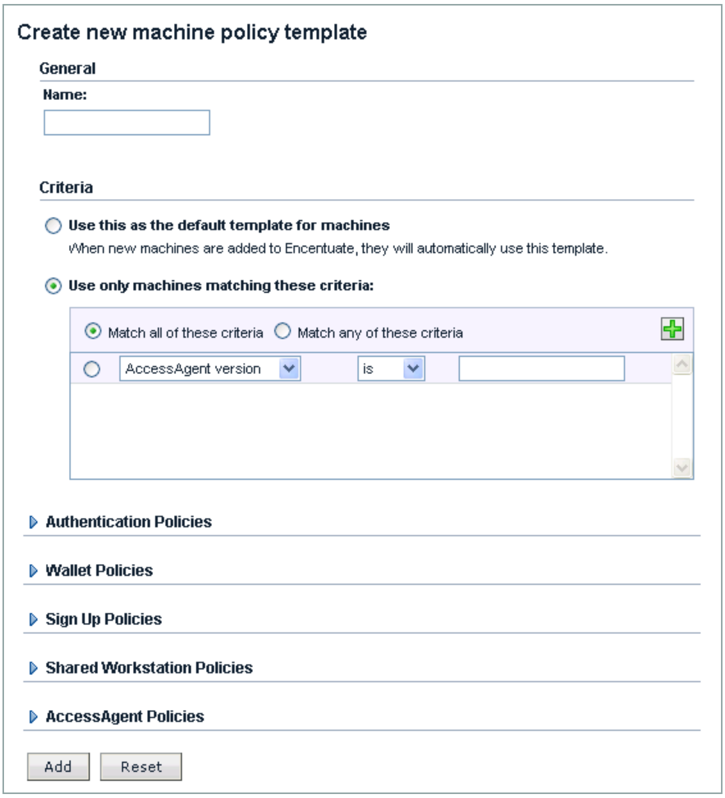
To create a machine template:

❶ Click *AccessAdmin >> Machine Policy Templates >> New template*.

❷ Enter a name for the new template and specify whether the machine policy template will be the default template, or whether it will be used by certain machines matching a specific criteria.

For more information on setting criteria, see Searching and managing machines, To set criteria:.

❸ Show the policies by clicking the arrow in the panel heading to expand them. You can modify any of these policies.



Create new machine policy template

General

Name:

Criteria

○ Use this as the default template for machines

When new machines are added to Encentuate, they will automatically use this template.

● Use only machines matching these criteria:

● Match all of these criteria ○ Match any of these criteria

○ AccessAgent version | is |

Enter machine policy name, set criteria, and click Add

4. When you have finished making your selections, click Add. The new template will appear in the AccessAdmin navigation panel on the left side of the browser.

   If you have changed your mind and no longer want to create a new template, click Reset.

Modifying a template

To modify a policy template:

1. In the AccessAdmin navigation panel, select *User Policy Templates or Machine Policy Templates >> [name of template]*.

2. Show the policies by clicking the arrow in the panel heading to expand it. You can modify any of these policies.

3. When you have finished making your selections, click Update.

   If you have changed your mind and no longer want to modify the template, click Reset.

Deleting a template

If a template is no longer used, you can delete it.

To delete a template:

❶ In the AccessAdmin navigation panel, select *User Policy Templates or Machine Policy Templates >> [name of template].*

❷ Scroll down to the bottom of the page and click Delete.

Applying policy templates to users

Policy templates can be applied to users during sign up or by using AccessAdmin.

Applying policy templates during sign up

IMS automatically applies policy templates to users upon sign up. There can be multiple policy templates defined in an IMS. One of these templates is set as default.

During user sign up, IMS checks the user attributes and chooses the policy template to apply. If there is no policy template that matches the attributes of a new user, the default policy template will be applied.

The Administrator can specify the policy templates to apply to users according to certain attributes. For example, if the Administrator chooses “department” as the attribute, IMS can apply a specific template to all users in the engineering department, for example, and another template to all users in the sales department, etc.

By default, the user attribute value is matched with the values specified in policy template assignments. Note that values are CASE SENSITIVE.

If the user attribute value does not have an exact match, IMS will check if the suffix of the user attribute value matches any assignments. If the suffix of a user attribute value matches two or more assignments, IMS applies the first template that matches the user attribute value.

In an extreme case wherein there is no policy template defined in IMS at all, IMS will not set any user policies during sign up.

Applying policy templates using AccessAdmin

A policy template can also be applied to a single user or to a group of users using the user’s or group’s profile page in AccessAdmin.

Applying policy templates to machines

IMS automatically applies policy templates to machines once they join the IMS Server, which are then automatically synchronized with AccessAgent. There can be several machine policy templates defined in IMS. One of these templates is set as default.

Once a machine joins the IMS, IMS checks the machine's attributes against the specified criteria and assigns the matching machine policy template.

If the machine matches two or more machine policy templates, IMS assigns the first matching policy template from the list of templates. If there is no policy template that matches the attributes of a new machine, the default machine policy template will be applied.

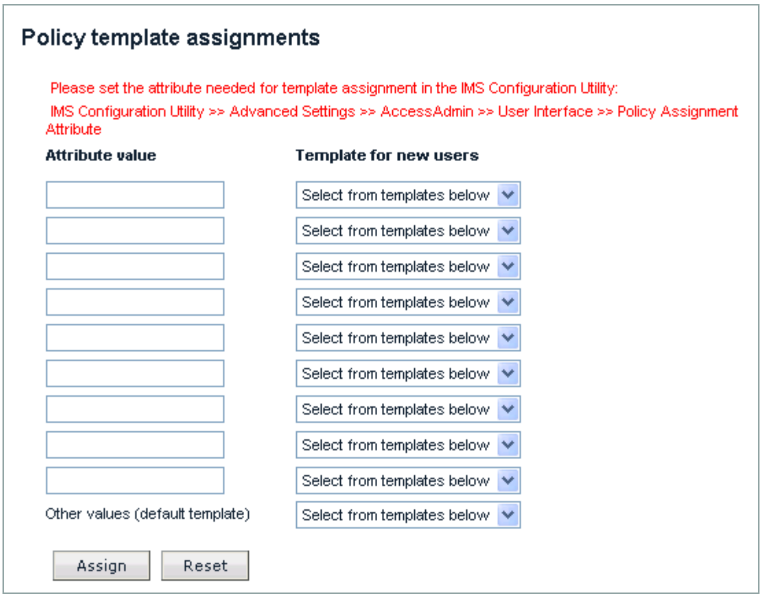
If a policy within a machine policy template is modified, all machines assigned to the machine policy template will get the new value. But if the criteria for machine policy template assignments are changed, existing assignments of machines to machine policy templates will not change.

Configuring user policy template assignments

To assign policy templates to new users during sign up, modify the IMS configuration file using the "encentuate.ims.ui.templateAsgAttribute" entry. This is the name of the user attribute in the enterprise directory whose value determines the policy template for each user.

You can also configure the attribute using IMS Configuration Utility. Go to *Advanced Settings >> AccessAdmin >> User Interface >> Policy assignment attribute*. See User interface in Using The IMS Configuration Utility for more information. Restart IMS after modifying the configuration.

You can then proceed to configure the mapping between the user attribute values and the policy template names using AccessAdmin. Go to *AccessAdmin >> User Policy Templates >> Template assignments*.



Policy template assignments

Please set the attribute needed for template assignment in the IMS Configuration Utility:
IMS Configuration Utility >> Advanced Settings >> AccessAdmin >> User Interface >> Policy Assignment Attribute

Attribute value	Template for new users
	Select from templates below
	Select from templates below
	Select from templates below
	Select from templates below
	Select from templates below
	Select from templates below
	Select from templates below
	Select from templates below
	Select from templates below
Other values (default template)	Select from templates below

Set the attribute value, select from the dropdown list, and click Assign

Searching and Managing Machines

This section discusses how to search and manage machines with Encentuate AccessAdmin.

This chapter covers the following topics:

- Searching for machines
- Managing machines

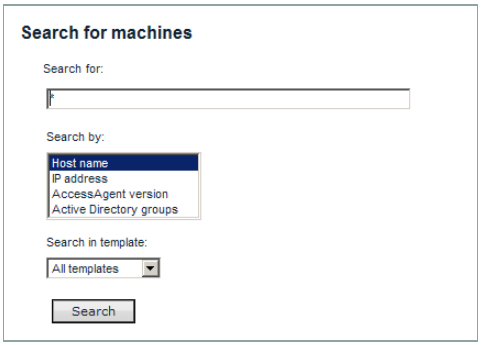
Searching for machines

There are two ways to search for machines:

- By attributes
- By template

To search by attributes:

1. Go to *Machines >> Search*.



Search for machines

Search for: *

Search by: Host name

Search in template: All templates

Enter the machine name or search by attribute or template

Enter an asterisk (*) in the **Search For** field to search from all machines.

2. Enter the machine attribute detail in the **Search for** field. If not, select a specific attribute under the **Search by** field and click **Search**. You can search for a machine by any of these four search attributes:

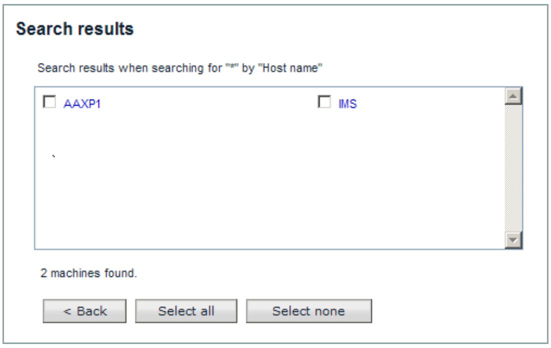
   Host name
   Enter the unique name or identification of your domain.

   IP address
   Specify the Internet Protocol address or the unique number assigned to your computer in a network.

   AccessAgent version
   Enter the version of the AccessAgent installed in your machine.

   Active Directory groups
   Select the Active Directory security group of your machine. A machine can belong to several groups. This criterion is satisfied as long as the machine is matches to at least one of the groups.

3. Click **Search**. The search results are displayed based on your selections/input:



Search results

Search results when searching for "*" by "Host name"

□ AAXP1 □ IMS

2 machines found.

Search results

To search by template:

1. Go to *Machines >> Search*.

2. Select a template from the **Search in template:** drop-down menu.

3. Click **Search**. The machines using the matching templates are displayed.

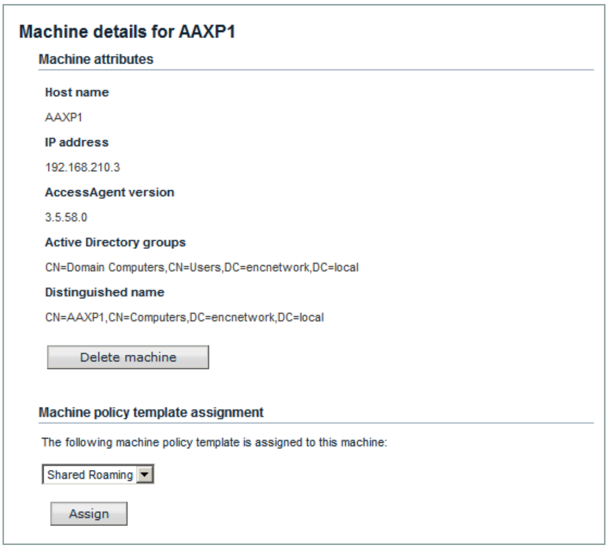
Managing machines

Viewing machine details

To view machine details:

1. Search for the machine either by attribute of by template.

2. In the **Search results** screen, click the machine name link. This displays the machine details for the machine you selected.



Machine details for AAXP1

Machine attributes

Host name

AAXP1

IP address

192.168.210.3

AccessAgent version

3.5.58.0

Active Directory groups

CN=Domain Computers,CN=Users,DC=encnetwork,DC=local

Distinguished name

CN=AAXP1,CN=Computers,DC=encnetwork,DC=local

Machine policy template assignment

The following machine policy template is assigned to this machine:

Shared Roaming

You can either delete a machine from here or assign a template

Assigning templates

To assign a template to a machine:

1. Search for the machine.

2. Click the machine name link.

3. Under **Machine policy template assignment**, select a template from the drop-down menu.

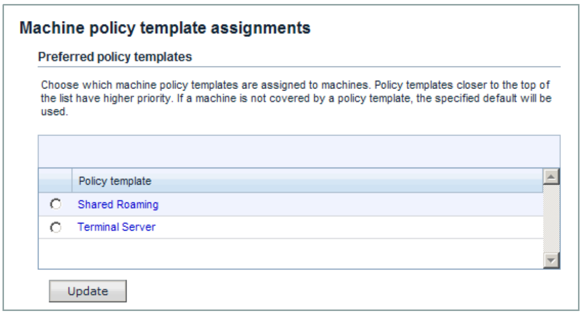
3. Click **Assign**.

Creating a new machine policy template

To create a new machine policy template:

❶ Go to *Machine Policy Templates >> Template assignments*.

❷ In *Machine policy template assignments >> Preferred policy template*, select the a policy template. Click the machine policy template link to view or configure details.



Machine policy template assignments

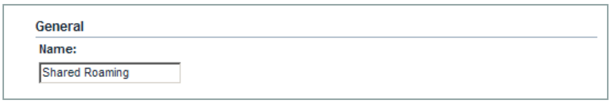
Preferred policy templates

Choose which machine policy templates are assigned to machines. Policy templates closer to the top of the list have higher priority. If a machine is not covered by a policy template, the specified default will be used.

	Policy template
○	Shared Roaming
○	Terminal Server

Assign a machine policy template

❸ In the **Machine policy template details** screen, enter your preferred machine name.

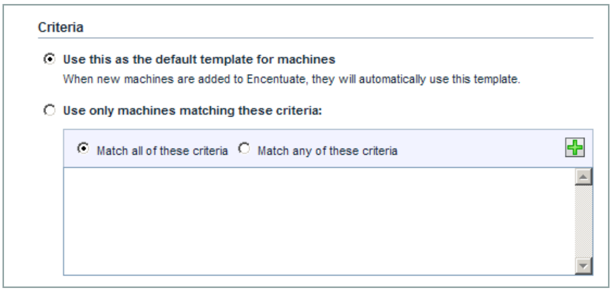


General

Name: Shared Roaming

Enter the machine policy template name

❹ Under **Criteria**, choose if you want to use the machine policy template as default of use it only if it matches a set of criteria.



Criteria

● **Use this as the default template for machines**

When new machines are added to Encentuate, they will automatically use this template.

○ **Use only machines matching these criteria:**

● Match all of these criteria ○ Match any of these criteria

Set the criteria

To set criteria:

1. Choose whether you want the machine filtered as they match **all** or **any** of the criteria. Select **Match all of these criteria** if you want to satisfy every search attribute criteria you have set. Select **Match any of these criteria** if you will settle for the search to match some and not all of the criteria you have set.

2. Click ➕ to add criteria fields and ✗ to delete. Select attribute options from the drop-down menu. Use the following comparison operators if:

   - **is**: the attribute is exactly what you want to search for

   - **is not**: you want to remove such attribute specification from the search

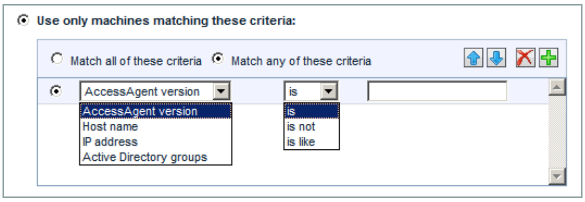
   - **is like**: is similar to the attribute you are looking for but not entirely the same.

   You can also use the following wildcard/character combinations in the criteria text box when using the **is like** option:

   abc - if you know what you are looking for, key-in the letters of your search string

   ***abc** - if you are not sure of the first letter but you know the succeeding letters of your search string

   abc* - if you know the first few letters of the search string except for the last letter



● Use only machines matching these criteria:

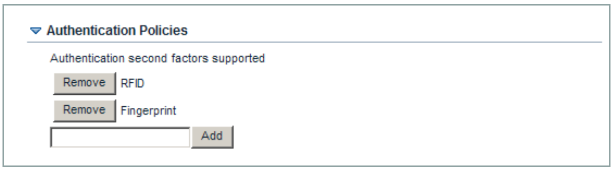
○ Match all of these criteria ● Match any of these criteria

● AccessAgent version ▾ is ▾

Specify criteria for machine screening

The order by which the criteria appear does not matter. The ↑ *and* ↓ *arrows are meant to make it easier for the administrator to put the criteria in his preferred order.*

3. Configure **Authentication Policies**.



▾ Authentication Policies

Authentication second factors supported

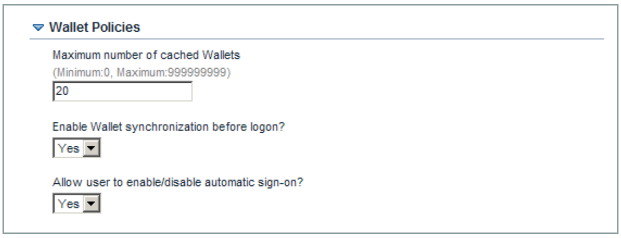
Remove RFID

Remove Fingerprint

Add

Add or remove supported second factors

4. Configure **Wallet Policies**.



Wallet Policies

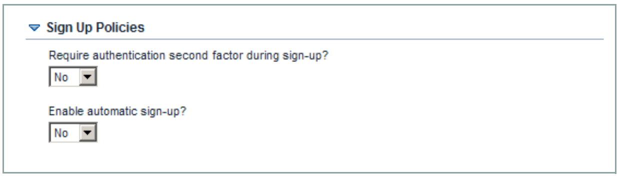
Maximum number of cached Wallets
(Minimum:0, Maximum:999999999)
20

Enable Wallet synchronization before logon?
Yes

Allow user to enable/disable automatic sign-on?
Yes

Specify Wallet policy settings

5. Configure **Sign Up Policies**.



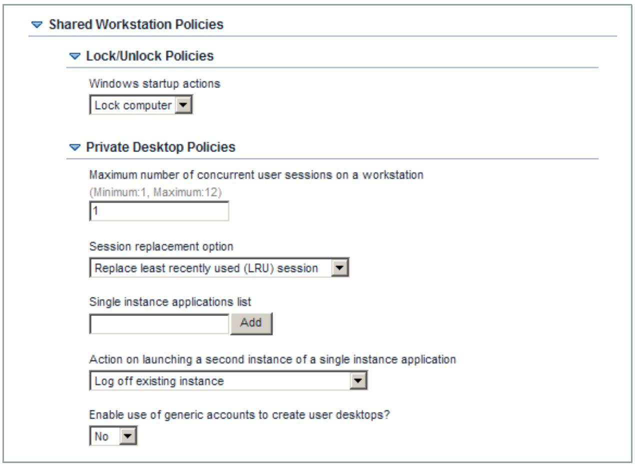
Sign Up Policies

Require authentication second factor during sign-up?
No

Enable automatic sign-up?
No

Specify sign-up policy settings

6. Configure **Shared Workstation Policies**.



Shared Workstation Policies

Lock/Unlock Policies

Windows startup actions
Lock computer

Private Desktop Policies

Maximum number of concurrent user sessions on a workstation
(Minimum:1, Maximum:12)
1

Session replacement option
Replace least recently used (LRU) session

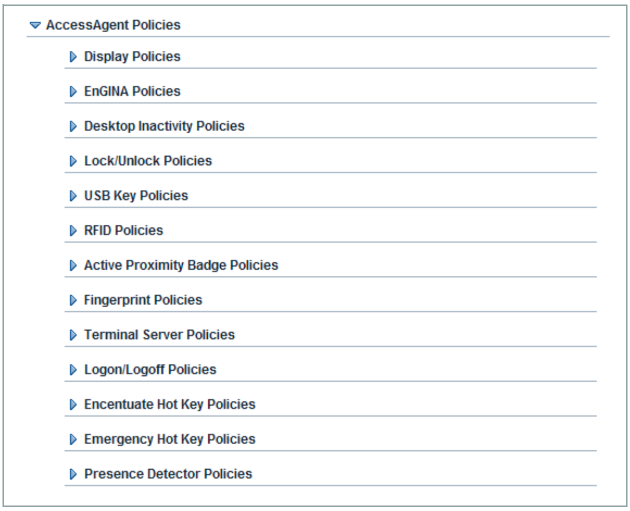
Single instance applications list

Action on launching a second instance of a single instance application
Log off existing instance

Enable use of generic accounts to create user desktops?
No

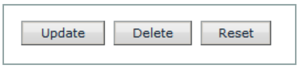
Specify shared workstation policy settings

7. Configure **AccessAgent Policies**.



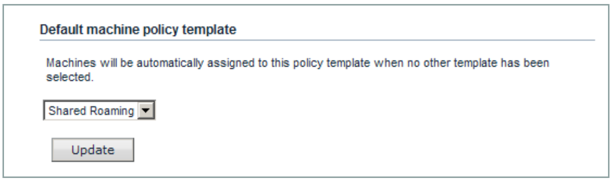
Click the arrows to expand and configure each AccessAgent policy

8. Click **Update** if you are satisfied with the changes. You can **Delete** or **Reset** the changes if required.



Click the appropriate button

❹ Select the **Default machine policy template** from the drop-down menu. Click **Update**.



Default machine policy template

Machines will be automatically assigned to this policy template when no other template has been selected.

Shared Roaming

Select the machine policy template from the dropdown menu

Reports and Audit Logs

This chapter discusses how to view system properties using Encentuate AccessAdmin, as well as to view and print audit reports. There are 2 ways to log on to AccessAdmin:

- Go to the console of the machine where the IMS Server is installed, access https://imsservername, and a logon prompt will be presented; or

- Log on to AccessAgent on any machine as Administrator, and then launch https://imsservername.

When logging on to AccessAdmin, enter the fully qualified domain name (for example, https://ims.encentuate.com).

If the IMS server is accessed without using the fully qualified domain name, AccessAgent will not be able to perform logon to search page automatically.

In the main user interface, you can find links to all the available administration functions. The main link, AccessAdmin, should be visible at all times. Click the link to view the AccessAdmin user interface.

This chapter covers the following topics:

- Viewing and printing audit logs

- Viewing and printing audit reports

- Integrating audit log database with a commercial reporting tool

- Tamper-evident audit logs

- Maintaining audit logs

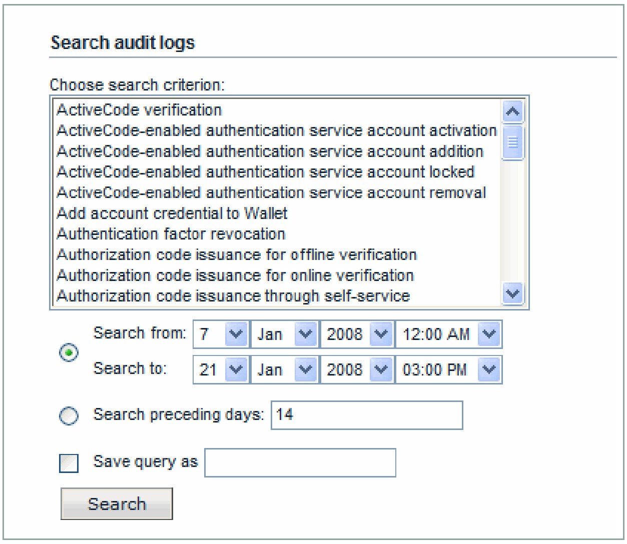
Viewing and printing audit logs

Using AccessAdmin, you can generate audit logs on one or more selected activities (e.g., authentication factor verification, authorization code issuance, etc.) within a specified time period.

The audit logs display the details of each activity, such as the user who performed the activity, the date and time of the activity, and the result of the activity.

To view and print audit logs:

❶ Click *AccessAdmin >> System >> Audit Logs*.



Search audit logs

Choose search criterion:

ActiveCode verification
ActiveCode-enabled authentication service account activation
ActiveCode-enabled authentication service account addition
ActiveCode-enabled authentication service account locked
ActiveCode-enabled authentication service account removal
Add account credential to Wallet
Authentication factor revocation
Authorization code issuance for offline verification
Authorization code issuance for online verification
Authorization code issuance through self-service

● Search from: 7 Jan 2008 12:00 AM
Search to: 21 Jan 2008 03:00 PM

○ Search preceding days: 14

□ Save query as

Generating audit logs

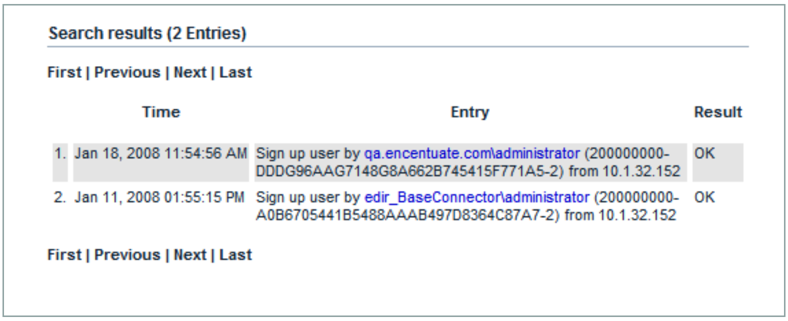
❷ Select an **Event** from the list by clicking on it. You can select multiple events by holding down the **Ctrl** key while clicking.

❸ Click the **Search From** radio button to specify the date range of the activity. Select a date, a month, a year, and a specific hour from the drop-down lists. Repeat with the **To** drop-down lists.

Alternatively, mark the **Search by preceding days** radio button, and enter a number in the respective field.

❹ If you want to save the search criteria for future retrieval, mark the **Save query as** checkbox and enter a file name.

❺ Click **Search**. The search results appear below the search fields.



Search results (2 Entries)

First | Previous | Next | Last

	Time	Entry	Result
1.	Jan 18, 2008 11:54:56 AM	Sign up user by qa.encentuate.com\administrator (20000000-DDDG96AAG7148G8A662B745415F771A5-2) from 10.1.32.152	OK
2.	Jan 11, 2008 01:55:15 PM	Sign up user by edir_BaseConnector\administrator (20000000-A0B6705441B5488AAAB497D8364C87A7-2) from 10.1.32.152	OK

First | Previous | Next | Last

Generating audit logs (search results)

Viewing and printing audit reports

Using AccessAdmin, you can generate audit reports that display a summary of user information, token information, application usage, and Helpdesk activity within a specified time period. Actions performed by users, Helpdesk officers, and Administrators are all logged in audit reports with a comprehensive audit trail.

Generating and printing user information reports

The user information report contain the specified user's (or users') activity, sorted by event, result, and time. The report also displays the users' machine IP address and the full name of the user (not just the Encentuate user name).

To generate and print user information reports:

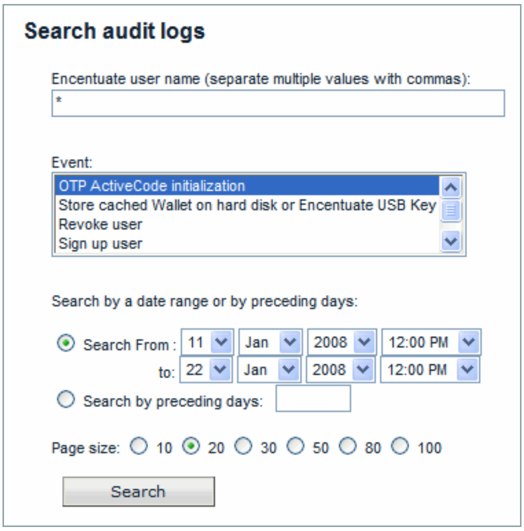
❶ Click *AccessAdmin >> Reports >> User information*.

❷ Enter the **Encentuate user name**(s) you want to generate the audit report for. You can enter one user name, several user names separated by commas, all user names starting with a particular letter or letters (for example, **c***, **bre***, etc.), or all user names (by typing an asterisk, *).

❸ Select an **Event** from the list by clicking on it. You can select multiple events by holding down the **Ctrl** key while clicking.

❹ Click the **Search From** radio button to specify the date range of the user activity. Select a date, a month, a year, and a specific hour from the drop-down lists. Repeat with the **To** drop-down lists.

Alternatively, click the **Search by preceding days** radio button, and enter a number in the respective field.



Search audit logs

Encentuate user name (separate multiple values with commas): *

Event:
- OTP ActiveCode initialization (selected)
- Store cached Wallet on hard disk or Encentuate USB Key
- Revoke user
- Sign up user

Search by a date range or by preceding days:

● Search From : 11 Jan 2008 12:00 PM
to: 22 Jan 2008 12:00 PM

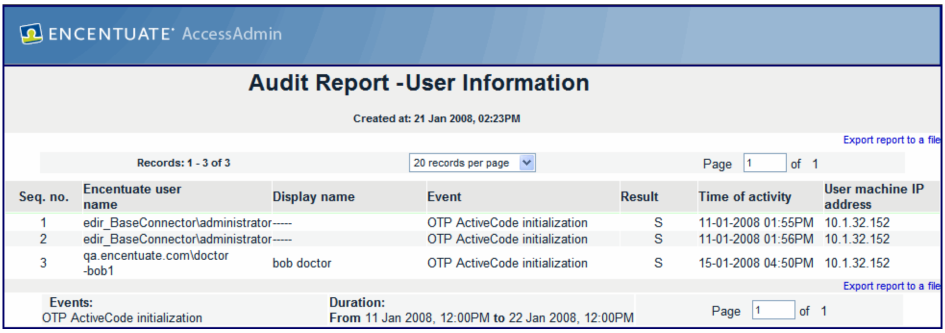
○ Search by preceding days:

Page size: ○ 10 ● 20 ○ 30 ○ 50 ○ 80 ○ 100

Generate user information report

5. Specify the **Page size** by clicking on a radio button representing the number of results you want AccessAdmin to display on one page.

6. Click **Search**. The report appears in a new browser window.



Audit Report -User Information

Created at: 21 Jan 2008, 02:23PM

Records: 1 - 3 of 3 20 records per page Page 1 of 1

Seq. no.	Encentuate user name	Display name	Event	Result	Time of activity	User machine IP address
1	edir_BaseConnector\administrator	-----	OTP ActiveCode initialization	S	11-01-2008 01:55PM	10.1.32.152
2	edir_BaseConnector\administrator	-----	OTP ActiveCode initialization	S	11-01-2008 01:56PM	10.1.32.152
3	qa.encentuate.com\doctor -bob1	bob doctor	OTP ActiveCode initialization	S	15-01-2008 04:50PM	10.1.32.152

Events:
OTP ActiveCode initialization

Duration:
From 11 Jan 2008, 12:00PM **to** 22 Jan 2008, 12:00PM

Page 1 of 1

User information report search result

7. You can generate the report by clicking **Print** in the browser's toolbar.

Generating and printing token information reports

A token information report contain the specified user's (or users') activity, sorted by token type, event, and time. The report also displays the users' machine IP address and the full name of the user.

To generate and print token information reports:

1. Click *AccessAdmin >> Reports >> Token information*.

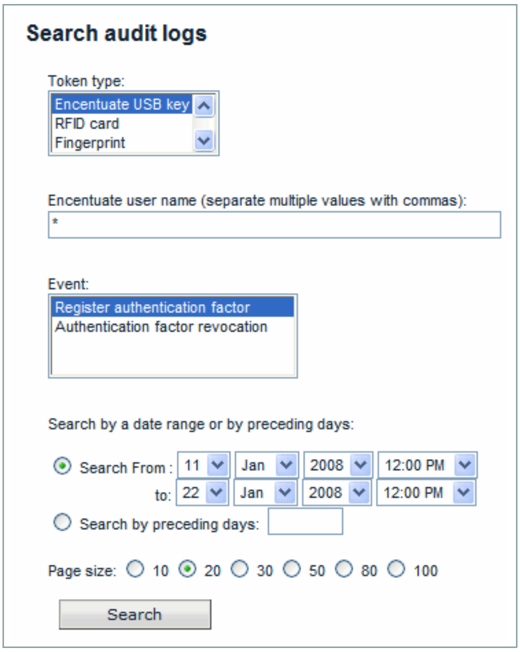
❷ Select a **Token type** from the list by clicking on it. You can select multiple token types by holding down the **Ctrl** key while clicking.

❸ Enter the **Encentuate user name**(s) you want to associate the tokens with. You can enter one user name, several user names separated by commas, all user names starting with a particular letter or letters (for example, **c***, **bre***, etc.), or all user names (by typing an asterisk, *).

❹ Select an **Event** from the list by clicking on it. You can select multiple events by holding down the **Ctrl** key while clicking.

❺ Click the **Search From** radio button to specify the date range of the user activity. Select a date, a month, a year, and a specific hour from the drop-down lists. Repeat with the **To** drop-down lists.

Alternatively, click the **Search by preceding days** radio button, and enter a number in the respective field.



Search audit logs

Token type:
- Encentuate USB key
- RFID card
- Fingerprint

Encentuate user name (separate multiple values with commas): *

Event:
- Register authentication factor
- Authentication factor revocation

Search by a date range or by preceding days:

● Search From : 11 Jan 2008 12:00 PM
to: 22 Jan 2008 12:00 PM

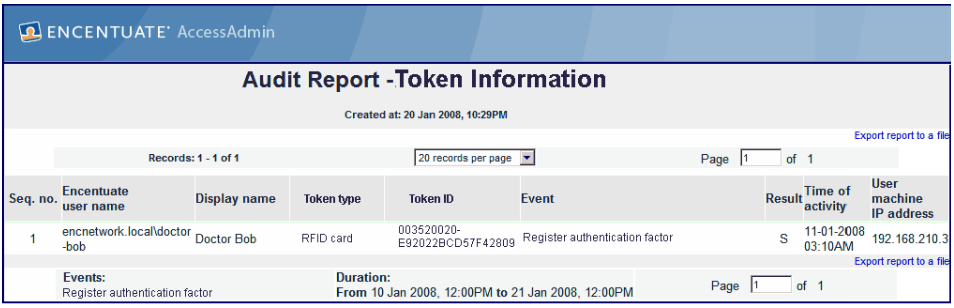
○ Search by preceding days:

Page size: ○ 10 ● 20 ○ 30 ○ 50 ○ 80 ○ 100

Generate token information report

❻ Specify the **Page size** by clicking on a radio button representing the number of results you want AccessAdmin to display on one page.

❼ Click **Search**. The report appears in a new browser window.



Audit Report -Token Information

Created at: 20 Jan 2008, 10:29PM

Export report to a file

Records: 1 - 1 of 1 | 20 records per page | Page 1 of 1

Seq. no.	Encentuate user name	Display name	Token type	Token ID	Event	Result	Time of activity	User machine IP address
1	encnetwork.local\doctor-bob	Doctor Bob	RFID card	003520020-E92022BCD57F42809	Register authentication factor	S	11-01-2008 03:10AM	192.168.210.3

Export report to a file

Events: Register authentication factor | Duration: From 10 Jan 2008, 12:00PM to 21 Jan 2008, 12:00PM | Page 1 of 1

Token information report search result

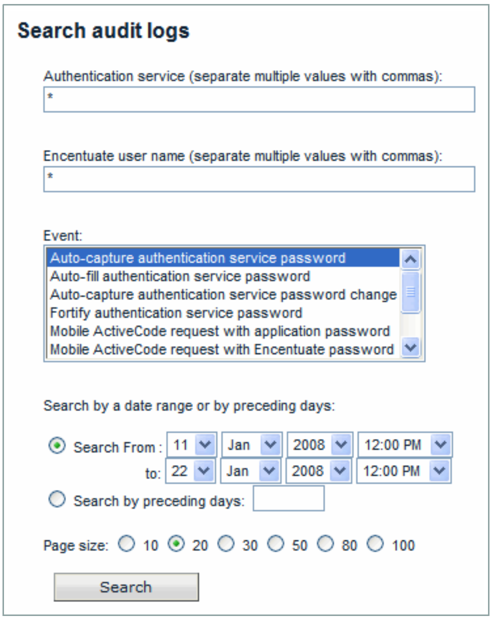
8 You can generate the report by clicking **Print** in your browser's toolbar.

Generating and printing application usage reports

You can generate an application usage report containing the specified user's (or users') authentication service activity, sorted by event, and time. The report also displays the users' machine IP address and the full name of the user.

To generate and print application usage reports:

1 Click *AccessAdmin >> Reports >> Application usage*.



Search audit logs

Authentication service (separate multiple values with commas): *

Encentuate user name (separate multiple values with commas): *

Event:
- Auto-capture authentication service password
- Auto-fill authentication service password
- Auto-capture authentication service password change
- Fortify authentication service password
- Mobile ActiveCode request with application password
- Mobile ActiveCode request with Encentuate password

Search by a date range or by preceding days:

● Search From : 11 Jan 2008 12:00 PM
to: 22 Jan 2008 12:00 PM

○ Search by preceding days:

Page size: ○ 10 ● 20 ○ 30 ○ 50 ○ 80 ○ 100

Generate application usage report

❷ Enter an **Authentication service**. You can enter one user authentication service, several authentication services separated by commas, all authentication services starting with a particular letter or letters (for example, **c***, **yah***, etc.), or all authentication services (by typing an asterisk, *)

❸ Enter the **Encentuate user name**(s) you want to associate the authentication service(s) with. You can enter one user name, several user names separated by commas, all user names starting with a particular letter or letters (for example, **c***, **bre***, etc.), or all user names (by typing an asterisk, *).

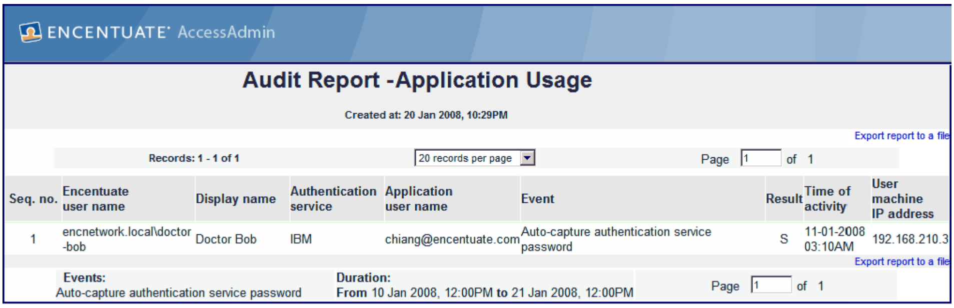
❹ Select an **Event** from the list by clicking on it. You can select multiple events by holding down the **Ctrl** key while clicking. You can scroll down to find more events down the list.

❺ Click the **Search From** radio button to specify the date range of the user activity. Select a date, a month, a year, and a specific hour from the drop-down lists. Repeat with the **To** drop-down lists.

Alternatively, click the **Search by preceding days** radio button, and enter a number in the respective field.

❻ Specify the **Page size** by clicking on a radio button representing the number of results you want AccessAdmin to display on one page.

❼ Click **Search**. The report appears in a new browser window.



Audit Report -Application Usage

Created at: 20 Jan 2008, 10:29PM

Export report to a file

Records: 1 - 1 of 1 | 20 records per page | Page 1 of 1

Seq. no.	Encentuate user name	Display name	Authentication service	Application user name	Event	Result	Time of activity	User machine IP address
1	encnetwork.local\doctor-bob	Doctor Bob	IBM	chiang@encentuate.com	Auto-capture authentication service password	S	11-01-2008 03:10AM	192.168.210.3

Export report to a file

Events: Auto-capture authentication service password

Duration: From 10 Jan 2008, 12:00PM to 21 Jan 2008, 12:00PM

Page 1 of 1

Application usage report search result

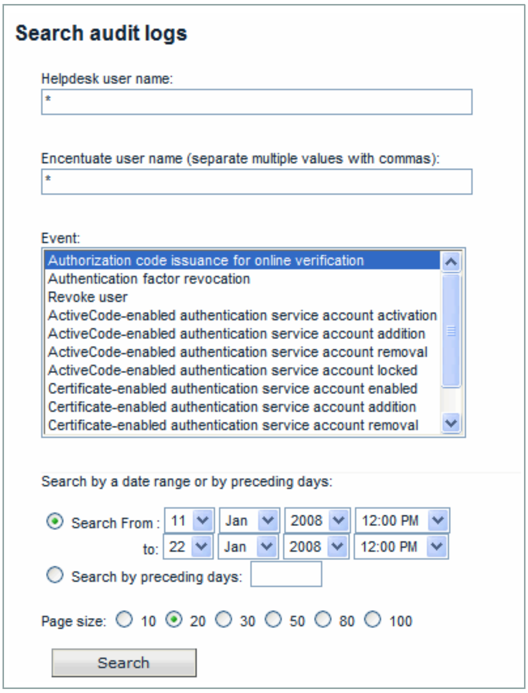
❽ You can generate the report by clicking **Print** in your browser's toolbar.

Generating and printing Helpdesk activity report

You can generate a Helpdesk activity report in relation to specific user's (or users') action, sorted by event, and time. The report also displays the users' machine IP address, token type, token ID, and the full name of the user. Token type and token ID information will only be displayed if they are available.

To generate and print Helpdesk activity reports:

1. Click *AccessAdmin >> Reports >> Helpdesk activity.*



Search audit logs

Helpdesk user name:
*

Encentuate user name (separate multiple values with commas):
*

Event:
Authorization code issuance for online verification
Authentication factor revocation
Revoke user
ActiveCode-enabled authentication service account activation
ActiveCode-enabled authentication service account addition
ActiveCode-enabled authentication service account removal
ActiveCode-enabled authentication service account locked
Certificate-enabled authentication service account enabled
Certificate-enabled authentication service account addition
Certificate-enabled authentication service account removal

Search by a date range or by preceding days:

● Search From : 11 Jan 2008 12:00 PM
to: 22 Jan 2008 12:00 PM
○ Search by preceding days:

Page size: ○ 10 ● 20 ○ 30 ○ 50 ○ 80 ○ 100

Search

Generate Helpdesk activity report

2. Enter the **Helpdesk user name**(s) you want to associate the tokens with. You can enter one user name, several user names separated by commas, all user names starting with a particular letter or letters (for example, **c***, **ale***, etc.), or all user names (by typing an asterisk, *).

3. Enter the **Encentuate user name**(s) you want to associate the Helpdesk officer with. You can enter one user name, several user names separated by commas, all user names starting with a particular letter or letters (for example, **c***, **bre***, etc.), or all user names (by typing an asterisk, *).

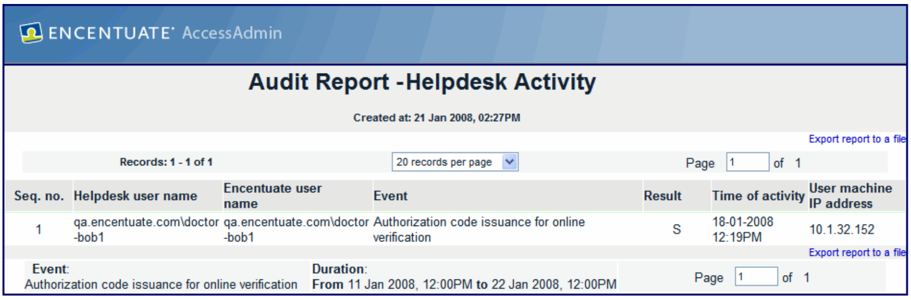
4. Select an **Event** from the list by clicking on it. You can select multiple events by holding down the **Ctrl** key while clicking. You can scroll down to find more events down the list.

5. Click the **Search From** radio button to specify the date range of the user activity. Select a date, a month, a year, and a specific hour from the drop-down lists. Repeat with the **To** drop-down lists.

   Alternatively, click the **Search by preceding days** radio button, and enter a number in the respective field.

6. Specify the **Page size** by clicking on a radio button representing the number of results you want AccessAdmin to display on one page.

7. Click **Search**. The report appears in a new browser window.



Audit Report -Helpdesk Activity

Created at: 21 Jan 2008, 02:27PM

Seq. no.	Helpdesk user name	Encentuate user name	Event	Result	Time of activity	User machine IP address
1	qa.encentuate.com\doctor-bob1	qa.encentuate.com\doctor-bob1	Authorization code issuance for online verification	S	18-01-2008 12:19PM	10.1.32.152

Event:
Authorization code issuance for online verification

Duration:
From 11 Jan 2008, 12:00PM to 22 Jan 2008, 12:00PM

Application usage report search result

8. You can generate the report by clicking **Print** in your browser's toolbar.

Integrating audit log database with a commercial reporting tool

This section illustrates the process of integrating the Encentuate audit log database with third party commercial reporting tools, such as Crystal Reports, Eclipse.

To integrate an audit log database with a commercial reporting tool:

1. Run `nwRptUsr.bat` from `imsserver\ims\bin`.

   The CLT creates a new database user called IMS Reports User that has read-only access to the IMS views. In order to run it, you need the Administrator password for the database (usually called 'sa').

   It has the following usage pattern:

```
nwRptUsr.bat --adminUser value --adminPass value --reportsUser
value --reportsPass value

      -h ......................help

      -v ......................version

     --adminUser value.......The database Administrator account
username.

     --adminPass value.......The database Administrator account
password.

      --reportsUser value.....The IMS Reports User account
username that is to be created.

      --reportsPass value.....The IMS Reports User account
password that will be set.
```

2. Have the following information to configure the SQL Reporting Tool to access the views:

   - The database user name and password.
   - The database connection parameters or strings.
   - Information on the schemas of the exposed SQL views.

Tamper-evident audit logs

The IMS Server logs various types of activities, such as web service invocation, user administration activities and user AccessAgent activities.

Audit logs are susceptible to tampering, but you can protect them by turning on the hashing of the log, or usually referred to as **log-signing**.

To turn on hashing, you must modify a configuration key in **ims.xml** using the IMS Configuration Utility. For details on how to modify the configuration key, see the section on Modifying the IMS configuration keys (basic settings).

The following activity logs can be made tamper-evident by log-signing:

- System management activity
- System operations
- User administration activity
- User activity
- User service

You can enable only those activities that you want to make tamper-evident.

Checking for evidence of audit log tampering

To ensure the integrity of an audit log, you can follow the procedures outlined in this section.

Running the checking batch file

To check whether there is any tampering in your log, you can run the log verifier batch file: `imsserver\bin\vrfyLogs.bat`.

The batch file can be used as:

```
vrfyLogs.bat -s <imsServer>  [-t <logTable>]   [-f
<outputFileFormat>][-o  <outputFile>]
```

where

- “imsServer” is the name of the computer where the IMS server is residing. For example: “encentuateims”.
- “logActivity” is the name of activity log to be verified. For example, “logUserService” is used to verify IMS web service activities. If you want to verify all types of activities, you can also specify “ALL”. This parameter is optional. The default value is “ALL”.
- “outputFileFormat” is the default format of the output file for log verification.You can either specify “xml” or “txt”. This parameter is optional. The default value is “txt”.
- “outputFile” is the location of the result file. This parameter is optional. If it is not specified, the log verifier uses the default directory.

The verification result is in a file with current date, which can be found in imsserver\logs\date\logVeriResult2005090916.xml.

Date indicates the date that the batch file was run.

Interpreting the output file

The log verifier provides a report of verification activity in the form of a file, which can be a text file or an XML file. The report is saved in the same directory as the log verifier: imsserver\bin. The name of the file can be in one of the following formats:

Text file format

logVerifierLog20041119.txt

The format is: “logVerifierLog” + year + month + date + “.txt”

Text file with no evidence of tampering

The report lists the section start and end log ID, the total number of records in the section, followed by the individual record verification. It also provides the record verification for each record and gives the status of the record, i.e, whether or not the record has been tampered with.

Each section also has the integrity result of the whole section in order to find out if there is any deletion in the beginning or the end.

```
Server ID: lily
Started Verifying the Logs from Database
2005-09-14 14:28:16
Log Table            : IMSLOGUserActivity

Verifying section
Starting logId       : 342247(14/09/2005 02:28:15PM)
Total records        : 50

Verifying Records
Starting logId        : 342247(14/09/2005 02:28:15PM)
Ending logId          : 342296(14/09/2005 02:28:15PM)

No of hashed records processed   : 50

Record Status        : No tampering detected for the records in
the section.
Integrity status      : This section is intact. There are no
tampered records.
```

Sample of output file: Text

Text file with evidence of tampering

If the logs have been tampered and the log verification information is initialized, the report will contain two categories: one for the records which integrity cannot be verified, and another that consists of records that have not been tampered with.

The following sample report contains the two categories of verified logs.

```
Server ID: lily
Started Verifying the Logs from Database
2005-09-14 14:28:30
Log Table                 : IMSLOGUserActivity

Verifying section
Starting logId            : 343047(14/09/2005 02:28:29PM)
Ending logId              : 343147(14/09/2005 02:28:30PM)
Total records             : 50

Verifying Records
Starting logId            : 343047(14/09/2005 02:28:29PM)
Ending logId              : 343047(14/09/2005 02:28:29PM)

No of hashed records processed   : 1

Record Status             : The first record was tampered or
cannot be verified. Records had possibly been deleted from the
beginning.
```

Sample of output file with evidence of tampered records: Text

```
No of hashed records processed   : 24

Record Status              : No tampering detected for the
records in the section.

Starting logId            : 343072(14/09/2005 02:28:29PM)
Ending logId              : 343081(14/09/2005 02:28:29PM)

No of hashed records processed   : 10

Record Status             : Records in the section had been
tampered

Starting logId            : 343082(14/09/2005 02:28:29PM)
Ending logId              : 343147(14/09/2005 02:28:30PM)

No of hashed records processed   : 15

Record Status              : No tampering detected for the
records in the section.

Integrity status           : The integrity of the records in the
section cannot be guaranteed. Records in the section had been
changed, or deleted.

Verifying Records
Starting logId            : 343147(14/09/2005 02:28:30PM)
Ending logId              : 343196(14/09/2005 02:28:30PM)

No of hashed records processed   : 50

Record Status            : No tampering detected for the records
in the section.

Integrity status          : This section is intact. There are no
tampered records.
```

Sample of output file with evidence of tampered records: Text

XML file format

logVerifierLog20041119.xml

The format is: “logVerifierLog” + year + month + date + “.xml”

The file names tells the user that the log verifier was run on “November 19, 2004". If the log verifier is run twice on the same day, it will replace the older file. Therefore, Encentuate recommends that you rename or back up the older file before running the log verifier again.

XML file with no evidence of tampering

If the default file format for the output file is XML, see the following sample file:

```
<?xml version="1.0" encoding="UTF-8" ?>

   - <LogVerification>
   - <ImsServerId Name="lily">
   - <Table Name="IMSLOGUserService">
   - <LogSection>
   - <Start>
     <LogId>87989</LogId>
     <Time>14/09/2005 11:37:11AM</Time>
     </Start>
   - <End>
     <LogId>88038</LogId>
     <Time>14/09/2005 11:37:11AM</Time>
     </End>
     <TotalNoOfSignedRecords>50</TotalNoOfSignedRecords>
   - <RecordVerification>
   - <RecordSection>
   - <Start>
     <LogId>87989</LogId>
     <Time>14/09/2005 11:37:11AM</Time>
     </Start>
   - <End>
     <LogId>88038</LogId>
     <Time>14/09/2005 11:37:11AM</Time>
     </End>
     </RecordSection>
    <NoOfHashedRecordsProcessed>50</NoOfHashedRecordsProcessed>
     <Status>0</Status>
     <StatusDescription>No tampering detected for the records in
   the section.</StatusDescription>
     </RecordVerification>
   - <IntegrityVerificationForTheSection>
     <Status>0</Status>
     <StatusDescription>This section is intact. There are no
   tampered records.</StatusDescription> \
     </IntegrityVerificationForTheSection>
     </LogSection>
     </Table>
     </ImsServerId>
     </LogVerification>
```

Sample of output file: XML

XML file with evidence of tampering

When there is evidence of tampering, the XML output file will look like the following sample:

```
 <?xml version="1.0" encoding="UTF-8" ?> LogVerification>

- <ImsServerId Name="lily">

- <Table Name="IMSLOGUserService">

- <LogSection>

- <Start>
  <LogId>88589</LogId>
  <Time>14/09/2005 11:37:18AM</Time>
  </Start>

- <End>
  <LogId>88689</LogId>
  <Time>14/09/2005 11:37:18AM</Time>
  </End>
  <TotalNoOfSignedRecords>50</TotalNoOfSignedRecords>

- <RecordVerification>

- <RecordSection>

- <Start>
  <LogId>88589</LogId>
  <Time>14/09/2005 11:37:18AM</Time>
  </Start>

- <End>
  <LogId>88689</LogId>
  <Time>14/09/2005 11:37:18AM</Time>
  </End>
  </RecordSection>
  <NoOfHashedRecordsProcessed>50</NoOfHashedRecordsProcessed>
  <Status>0</Status>
  <StatusDescription>No tampering detected for the records in
the section.</StatusDescription>
  </RecordVerification>

 - <IntegrityVerificationForTheSection>
   <Status>5</Status>
   <StatusDescription>The integrity of the records in the
 section cannot be guaranteed. Individual records are valid, but
 record deletion had possibly happened at the end.</
 StatusDescription>
   </IntegrityVerificationForTheSection>
   </LogSection>
```

Sample of output file with evidence of tampered records: XML

```
- <LogSection>

- <Start>
  <LogId>88689</LogId>
  <Time>14/09/2005 11:37:18AM</Time>
  </Start>

- <End>
  <LogId>88738</LogId>
  <Time>14/09/2005 11:37:19AM</Time>
  </End>
  <TotalNoOfSignedRecords>50</TotalNoOfSignedRecords>

  <TotalNoOfSignedRecords>50</TotalNoOfSignedRecords>

- <RecordVerification>

- <RecordSection>

- <Start>
  <LogId>88689</LogId>
  <Time>14/09/2005 11:37:18AM</Time>
  </Start>

- <End>
  <LogId>88738</LogId>
  <Time>14/09/2005 11:37:19AM</Time>
  </End>
 </RecordSection>
  <NoOfHashedRecordsProcessed>50</NoOfHashedRecordsProcessed>
  <Status>0</Status>
  <StatusDescription>No tampering detected for the records in
the section.</StatusDescription>
  </RecordVerification>

- <IntegrityVerificationForTheSection>
  <Status>0</Status>
  <StatusDescription>This section is intact. There are no
tampered records.</StatusDescription>
  </IntegrityVerificationForTheSection>
  </LogSection>
  </Table>
  </ImsServerId>
  </LogVerification>
```

Sample of output file with evidence of tampered records: XML

Record status

There are individual record checks and whole-section integrity check.

The following record status are possible:

- There are no hashed records in the table

- No tampering detected for the records in the section
- No hashed record existed in the table.
- The first record was tampered or cannot be verified (records had possibly been deleted from the beginning)
- Records in the section had been tampered

For the final integrity check, the record status in XML file log and their meanings are as follows:

Status number	Description
0	The section is intact. There are no tampered records.
1	Log-hashing information was not detected in the database. This means that either the log-hashing information had totally been deleted, or log-hashing has never been enabled.
2	No hashed record was inserted after enabling log-hashing or after housekeeping.
3	The first record was tampered or cannot be verified. Records had possibly been deleted from the beginning.
4	The integrity of the records in the section cannot be guaranteed. Records had possibly been deleted from both ends.
5	The integrity of the records in the section cannot be guaranteed. Individual records are valid, but record deletion had possibly happened.
6	The integrity of the records in the section cannot be guaranteed. Records in the section had been changed, or deleted.
7	Tampering detected. Hashed records had all been deleted from the log table.

Record status in XML file log

Maintaining audit logs

Refer to this section to learn how to maintain your audit logs (also known as “housekeeping”), and how to determine when to prune logs to free disk space.

There are two ways maintain your audit logs. You can either run a batch file or schedule the housekeeping activity using the IMS Configuration Utility.

Running the maintenance batch file

Run imsserver/bin/hskpLogs.bat.

The usage of the batch file is:

```
hskpLogs.bat  -d <daysToKeep>]  [-i  <imsServer>]

                    [-m logSystemManagementActivity>]

                    [-p  <logSystemOps>]

                    [-u  <logUserActivity>]

                    [-a <logUserAdminActivity>]

                    [-s <logUserService>]

                    [-f  <outputFileFormat>]

                    [-o  <outputFile>]
```

where

- “daysToKeep” is used to delete the log records that are older than the number of days.
- “logSystemManagementActivity” is used to delete system management activity logs
- “logSystemOps” is used to delete system operation logs
- “logUserActivity” is used to delete user activity logs
- “logUserAdminActivity” is used to delete user administration activity logs
- “logUserService” is used to delete user service logs. If there is no table specified, logs for all activities will be pruned.
- “imsServer” identifies the IMS server for which log hashing information will be initialized. The IMS server must be offline in order to initialize its logs.
- “outputFileFormat” is the format of output file of the log verification. You can either specify “xml” or “txt”. This parameter is optional. The default value is “txt”.
- “outputFile” is the name of the file and the directory where the results of housekeeping activities are to be stored. This parameter is optional. If it is not specified, log housekeeper creates a default name: hskpLog.txt

Initializing housekeeping

You can initialize housekeeping information by specifying an IMS Server. The initialization will cause the hashing information to be initialized.

During initialization, the program will ask you whether you really want to initialize the server:

```
If you initialize logs for the server, all previous log-hashing
information for log integrity checking will be lost. The IMS
Server you want to initialize must also be offline. Do you
really want to initialize server with serverId: lily log: all?

>(yes/no):
```

When you enter **Yes**, it will start initializing the server.

Scheduling maintenance using IMS Configuration Utility

Audit log maintenance can be scheduled in the **ims.xml** file, using the IMS Configuration Utility. See the IMS Server housekeeping for more information.

Viewing the result files

Result files are generated in the **imsserver\logs\date** folder where the batch file is run. There are several types of result:

- The log verification result
- The housekeeping result
- The hashing information

The log verification result

Before doing housekeeping, IMS will perform log verification. The verification result for each server is stored in a file prefixed with server name and suffixed with the date the maintenance took place. For example, the verification result for "server1" in XML format is **\logs\2005-09-14\server12005091411.xml**.

The housekeeping result

The result of housekeeping is stored in a default file if it is not given as **hskpLog.txt**. It gives the housekeeping information and status.

The hashing information

This information is created to keep a record of the hashing.

If it is the initialization of a log, the file contains two rows of the hashing information before and after the initialization.

```
352460,0,RJJa+eJ8dADj2wKBcOOjtIFCwp0=,AXojoyqhu09Qp90qdCASoH
9VsSo=,YG/n8qfrfY4cpSqhERKFlWYa8Gw=,2005-09-16 16:55:28

352660,0,RJJa+eJ8dADj2wKBcOOjtIFCwp0=,RJJa+eJ8dADj2wKBcOOjtI
FCwp0=,LTIF0xnsHAtoBfiyEtrgNKDIuV4=,2005-09-16 16:55:30
```

Hashing information: Log initialization

If it is for pruned records, it contains the hashing information before the records were pruned and the after the records are pruned. It also has the total pruned number of records.

```
354510,0,RJJa+eJ8dADj2wKBcOOjtIFCwp0=,XTCZXaZqHktdIjN3gUsL/
BoDa8k=,lJBoZFVhxP68fQY0z24VoyX4AbE=,2005-09-16 17:01:39

354909,8VsCnPPD9CCymx7lC6BLw6eEnTc=,LCH6VYp9CQZsSFhGkOTLcj58
9bU=,XTCZXaZqHktdIjN3gUsL/
BoDa8k=,dA+35M78zsH9sRg3KQZ7U6s5h2M=,2005-09-16 17:01:48



total records: 104
```

Hashing information: Pruned records

Configuration Tips

This chapter provides useful information when configuring Encentuate IMS Server.

Switching to another IMS Server

To switch to a different IMS Server, the following operations should be performed on the client machine:

- Set the machine policy pid_ims_server_name by changing the value from AccessAdmin.
- Download the IMS Server certificate by running: C:\Program Files\Encentuate\SetupCertDlg.exe.
- Log off AccessAgent (if logged on).
- Stop the AccessAgent processes: AATray.exe, DataProvider.exe, and Sync.exe.
- Stop the SOCIAccess service (net stop sociaccess).
- Delete the entire C:\Program Files\Encentuate\Cryptoboxes folder (back-up the existing ones to another place if you intend to switch back to the original IMS Server).
- Restart the machine.

Restarting the machine with a missing machine Wallet will force AccessAgent to re-create the machine Wallet by downloading the latest policies and AccessProfiles from the current IMS Server.

- If you already have the Cryptoboxes for the IMS Server backed-up somewhere, you can switch to it by performing the following operations:
- Log off AccessAgent (if logged on).
- Stop the AccessAgent processes: AATray.exe, DataProvider.exe, and Sync.exe.
- Stop the SOCIAccess service (net stop sociaccess).
- Restore the Cryptoboxes folder for the IMS Server (back-up the existing ones to another place if you intend to switch back to the original IMS Server).
- Start the SOCIAccess service (net start sociaccess).
- Run C:\Program Files\Encentuate\AATray.exe.

Copying AccessProfiles between IMS Servers

AccessStudio can be used to copy all the AccessProfiles from one IMS Server to another:

- Set the machine **policy pid_ims_server_name** to the IMS Server where AccessProfiles are to be copied from.
- Run AccessStudio.
- Perform a "Download from IMS Server".
- Save to a file (.eas extension) and exit AccessStudio.
- Set the machine policy **pid_ims_server_name** to the target IMS Server.
- Run AccessStudio.
- Open the saved file.
- Perform an "Upload All to IMS Server".

Deleting a user without revoking

Once a user is revoked through AccessAdmin, the user name cannot be used anymore. Sometimes, it may be useful to delete a user without revoking it, so that the user name cannot be reused. This can be achieved through the following operation:

- Rename the user through AccessAdmin, by displaying the user's profile, modifying the user name (to some name that will not be used, e.g., "deleteduser94", and clicking **Update**.
- If desired, revoke the renamed user.
- Remove the original user's cached Wallets that may still be lingering around client PC's hard disks.

Alternatively, the **Delete user** button can be enabled on AccessAdmin by turning the feature on using the IMS Configuration Utility (*Advanced Settings >> AccessAdmin >> User Interface >> Delete User Button*).

Promoting a user to Administrator directly through the database

After sign up, a user does not take on the Administrator or Helpdesk role unless configured to take on the Administrator role during IMS Server installation. As such, a new Administrator is usually promoted to the Administrator role by existing Administrators through AccessAdmin.

However, if, for some reason, there are no more Administrators in the IMS database (e.g., the only Administrator has left the company and no one knows the Administrator password), existing users can be promoted to Administrator directly through the database as follows:

- Launch the database management UI (Needs user with database Administrator rights).
- Open the IMSIdentityUniqueAttribute table to read off the imsID that corresponds to the target user.
- Open the IMSIdentityRole table and set the roleID to 6 for the imsID identified earlier.

✓ *The roleID of* 6 *is defined for "ImsAdmin" in the "IMSRole" table.*

Alternatively, the IMS CLTs can be used:

- Launch command prompt and go to the <IMS Installation Folder>\ims\bin folder.
- Use `findAcct.bat <user name>` to obtain the imsID.
- Use `addImsRole.bat <imsID> ImsAdmin` to promote user to Administrator.

Enabling/disabling autoplay for removable drives

For AccessAgent, the installer no longer sets the NoDriveTypeAutoRun Windows registry entry. For USB Key deployments, this entry should be set in the DeploymentOptions.reg file of the installer.

Improving AccessAgent performance

The AccessProfiles can become very large data objects when they are parsed by the DataProvider process of AccessAgent. These data objects must be kept in memory. Removing unused AccessProfiles can speed up AccessAgent performance. This can be done using AccessStudio - just right-click on each unused AccessProfile and choose delete.

Specifying IMS DB user account

You should not specify the SA account as the IMS DB user account. If you do, the installation will fail. The IMS DB user account should be different from the SA account.

Configuring the ADAM server

You are recommended to read the ADAM Step-by-Step Guide from the Microsoft Download Center for detailed configuration instructions. The following paragraphs provide some quick tips on configuring ADAM so that the LDAP connector can connect to it using SSL.

Obtaining a certificate

To create a certificate, you must install IIS and Certificate Authority. This is done through *Control Panel >> Add/Remove programs >> Add/Remove Windows Components*. For information on how to install IIS, refer to Microsoft documentation. To install a Certificate authority, select the Certificate services check box.

IIS should be installed before or at the same time as you install the certificate services.

Once the installation is complete, request a certificate by browsing the following URL using Internet Explorer: http://localhost/certsrv.

To obtain a certificate:

❶ Click **Request a certificate**.

❷ Click **Advanced certificate request**.

❸ Click **Create and submit a request to this CA**.

4. In the **Name** text box, enter the full-qualified DNS name of the server.
5. Make sure **Type of certificate** is **Server authentication certificate**
6. Select **PCKS10** as the format.
7. Optionally fill in the other information.
8. Click the **submit** button.

You have now created a certificate request.

To create a certificate, process the request as follows:

1. Open *Control Panel >> Administrative Tools >> Certification Authority*.
2. Browse to the **Pending requests** folder.
3. Locate the certificate request, right-click and select *All tasks >> issue*.

The certificate has now been created and it should reside in the "Issued certificates" folder. Now download and install the certificate:

1. Go to http://localhost/certsrv.
2. Click **View the status of a pending certificate request**.
3. Click the certificate request.
4. Click the certificate to install it.

Using the certificate with the ADAM service

To configure the ADAM service to use the certificate, you must put the certificate in the ADAM service's personal store as follows:

1. Click *Start >> Run*, and enter **mmc** to launch the Microsoft Management Console.
2. Click *File >> Add/Remove* snap-in.
3. Click **Add...** and select **Certificates**.
4. Select **Service account**.
5. Select **Local computer**.
6. Select your ADAM instance service.

7. Add a new **Certificate** snap-in, but this time, select **My user account** instead of **Service account**.

8. Click **Close** and **OK**.

9. Open the **Personal** folder under the **Certificates - Current user** tree

10. Select the certificate and copy it into the same location under **Certificates - adam instance name**.

11. Give the ADAM service account read permissions to the key under **C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys**

> *If these permissions are not set correctly, you will get an error in the event log: Schannel ID: 36870 – "A fatal error occurred when attempting to access the SSL server credential private key. The error code returned from the cryptographic module is 0x6."*

12. Restart your ADAM instance.

Verifying that SSL is working

To verify that SSL is working with ADAM:

1. Run the ADAM Tools Command Prompt from your ADAM program group.

2. Type **ldp** and click **Enter**.

3. Click *Connection >> Connect...*

4. Type the fully-qualified DNS name of your server in the server text box ("localhost" will not work as the DNS name is checked against the certificate).

5. Enter the SSL port of your ADAM installation (636 or 50001, or whatever you chose during the installation of ADAM).

6. Select the **SSL** check box and click **OK**.

7. If the installation was successful, you should get a lot of text in the right window and be able to bind using the *Connection >> bind...* functionality.

Running ADAM service with a domain user account

To run the ADAM service with a domain user account:

❶ If you intend to use a non-administrative domain user account (say, ”domainUser1”) as the ADAM service account, make sure the following steps are performed:

❷ Log on to Windows as “domainUser1” when requesting a server authentication certificate.

❸ In the certificate request page, mark the private key exportable.

❹ After installing the generated certificate into domainUser1’s personal certificate store, open Certificates snap-in and export that certificate with private key.

❺ Log on to Windows as Administrator and use Certificates snap-in to import the certificate into ADAM service instance personal certificate store.

❻ When granting “domainUser1” Read permission on private keys in C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys, set permission individually for each file as the permission on folder MachineKeys is not inherited.

Importing the root CA certificate into IMS Server trust store

For IMS Server to trust the ADAM server when establishing an SSL connection to it, the root CA certificate used to sign ADAM server certificate needs to be imported into the IMS Server trust store. The import can be done by executing the following command:

```
keytool -import -file <path_to_exported_certificate> -keystore
<path_to_ims_keystore> -alias <any_name> -storepass <password>
```

Restart IMS Server after the certificate is imported.

Turning off authentication for AccessAdmin

AccessAdmin is, by default, protected using SCR, which is a certificate-based authentication mechanism supported by AccessAgent. Hence, an Administrator must log on to AccessAgent first in order to access AccessAdmin.

For development or test IMS Servers, you may want to turn off authentication for AccessAdmin so as to simplify the configuration process. However, this should never be done for production IMS Servers.

To turn off authentication for AccessAdmin:

❶ Use the SQL Enterprise Manager (or equivalent tool) to insert the following data into the respective IMS database tables:

imsID=IMSADMIN1 into the IMSIdentity table

sociID=IMSADMINSID1 and imsID=IMSADMIN1 into the IMSSoci table

msID=IMSADMIN1 and roleID=6 into the IMSIdentityRole table

❷ Modify the web.xml file in <IMS Installation Folder>\ims\WEB-INF folder. Search for the following filter-mapping sections:

```
    <filter-mapping>

        <filter-name>ScrFilter</filter-name>

        <url-pattern>/*</url-pattern>

    </filter-mapping>

<!–

    <filter-mapping>

        <filter-name>NoAuthFilter</filter-name>

        <url-pattern>/ui/admin/*</url-pattern>

    </filter-mapping>

-->
```

❸ Comment out the “ScrFilter” and uncomment the “NoAuthFilter”. The sections should now look like this:

```
<!–

    <filter-mapping>

        <filter-name>ScrFilter</filter-name>

        <url-pattern>/*</url-pattern>

    </filter-mapping>

-->

    <filter-mapping>
```

```
            <filter-name>NoAuthFilter</filter-name>

            <url-pattern>/ui/admin/*</url-pattern>

        </filter-mapping>
```

4. Save the modified web.xml file.

5. Restart the IMS Server.

6. You should now be able to access the AccessAdmin UI without having to log on to AccessAgent.

Configuring the IMS Server download port

If IIS or some other Web servers are installed on the same machine as the IMS Server, it may be necessary to use a download port that is different from the default port 80. Configuration changes must be done on both the IMS Server and AccessAgent.

The IMS Server HTTP port must be changed from 80 to the desired port (e.g., 88) in the server.xml file located at <IMS Installation Folder>\conf\server.xml. In the section regarding the service 'tomcat-standalone', the following change (in boldface) should be made. Restart the IMS Server after the change is done.

```
<Connector
className="org.apache.coyote.tomcat4.CoyoteConnector"

  port="88" minProcessors="5" maxProcessors="75"

  enableLookups="false" redirectPort="443"

  acceptCount="100" debug="0"

  connectionTimeout="20000"

  useURIValidationHack="false"

  disableUploadTimeout="true" />
```

Modify the ImsDownloadPortDefault entry in the SetupHlp.ini file of the AccessAgent installer, then install AccessAgent. Alternatively, if AccessAgent has already been installed, you can modify the registry key [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\IMSService\DefaultIMSSettings] " ImsDownloadServicePort".

If there are existing cached Wallets, you will must delete those.

To delete cached Wallets:

1. Log off AccessAgent (if logged on).

2. Stop the AccessAgent processes: AATray.exe, DataProvider.exe, and Sync.exe.

3. Stop the SOCIAccess service (net stop sociaccess).

4. Delete the entire C:\Program Files\Encentuate\Cryptoboxes folder.

5. Restart machine.

Enabling RFID readers for AccessAgent running in VMware

Since the RFID reader is actually a Human Interface Device (HID), the following line should be added to the VMware image's VMX file: usb.generic.allowHID = "TRUE"

Modifying AccessAdmin web pages

Starting from IMS Server 3.5.0, JSPs are pre-compiled when an IMS Server is installed or upgraded. This is to improve the loading speed of IMS Server pages (AccessAdmin and IMS Configuration Utility) on first access.

Since the JSPs are pre-compiled, they cannot be edited or replaced without re-starting the IMS Server. Furthermore, the compiled JSP class also needs to be replaced and IMS Server needs to be re-started for the change to take effect.

Alternatively, you can exclude any of the JSPs from the pre-compilation requirement by modifying the <IMS Installation Folder>\ims\WEB-INF\web.xml file as follows:

1. Search, in web.xml, for the JSP file that you want to modify (e.g., indexAlt.jsp).

2. Comment out the entire servlet-mapping section for the JSP file by adding "<!--" at the beginning and "-->" at the end. For example:

   ```
   <!--<servlet-mapping>

             <servlet-name>ui.indexAlt_jsp</servlet-name>

        <url-pattern>/ui/indexAlt.jsp</url-pattern>

   </servlet-mapping>-->
   ```

3. Save the modified web.xml file and restart the IMS Server.

Troubleshooting

This chapter discusses the different problems you may encounter while using and configuring Encentuate IMS Server and how to deal with them.

IMS Server installation-related problems

Here some reasons why an Encentuate IMS Server installation can fail:

Specified information could not be verified

If you encounter the following message,

```
The specified information could not be verified. Please check
the specified values and ensure that SQL Server has SQL
Authentication enabled. Do you want to continue?
```

it is because the database is not set up correctly. Check that there is TCP listener at the database port you specified in the database configuration screen by using the command `netstat -a -p tcp` and see that there is a `<hostname>:1433` entry in the output.

Authentication factor could not be registered

If registration fails it could be due to any of the following reasons:

- The server name is not resolvable. It could be that it is not updated to the DNS.
- A valid server name is specified but it is different than the one specified during the IMS Server installation (for example DNS name vs. NetBIOS name).
- You are using an Internet proxy which requires authentication. AccessAgent does not prompt you to authenticate to the proxy, so authentication will fail. Proxy servers typically cache sessions so the problem can be solved by authenticating separately to the proxy server.

  The IMS Server may not be up. To verify that the IMS Server is up, go to `https://hostname`, where *hostname* is the name of the computer on which the IMS Server is installed.

You can see the IMS Server user interface page without getting prompted about untrusted SSL certificates.

SQL authentication not enabled

If you are prompted that SQL authentication should be enabled, do the following:

❶ Open the Enterprise Manager of the SQL Server.

❷ Go to *Tools >> SQL Server Configuration Properties*.

❸ Go to the Security tab and select SQL Server and Windows Authentication.

Default password for Sa not changed

To change the password for Sa:

❶ Open the Enterprise Manager.

❷ Go to the Security folder in the left panel.

❸ Click Logins.

❹ Right-click on the Sa icon and go to Properties to change the password.

USB Key is pre-initialized

If you are prompted that the USB Key is pre-initialized it means it is not a new USB Key. You must get a new USB Key and try again.

USB Key has been locked

An Encentuate USB Key gets locked after five incorrect entries of the password. You will must get a new USB Key to resume installation.

DLLs not accessible

If you restart the computer after the IMS Server installation fails and try to install again, the installation fails again because some DLLs are not accessible. This is because the IMS Server is partially installed and once the computer starts, the IMS service also starts up and the installer is not able to access the required DLLs. The IMS Service should be stopped before continuing with the installation.

Incorrect database configuration

IMS Server installation may fail due to the following reasons:

Database server has been configured to return No Count

As the IMS Server depends on these counts to determine the success or failure of database operations, it is necessary to disable this database feature.

To disable the database feature:

1. In Enterprise Manager, right-click on database server and select Properties.
2. Go to *Connection* > *No Count*, and disable it.

Database user privileges are incorrect

The database user should have public, db_owner rights for the IMS database. The user should not be a DB Administrator account.

To check whether the database user has the correct privileges:

1. In Enterprise Manager, click on *DB Server* > *Security* > *Logins*.
2. Right-click on **DB login** and select **Properties**.
3. Click on **Server Roles** tab.
4. Make sure that **System Administrators** and **Database Creators** roles are unchecked.

Checking the installed version of IMS Server

See Checking the IMS Server status and version to find out how to check the installed version of the IMS Server.

Running the IMS Server console

By default, the IMS Server is run automatically as a service “IMSService” when the server starts up. When run in this mode, it may be difficult to troubleshoot any problems with the IMS Server. Alternatively, IMS Server can be run in console mode so that error messages, if any, are displayed on the fly.

To run IMS Server in console mode:

❶ Stop the IMSService (net stop IMSService).

❷ Run the batch file: <IMS Installation Folder>\ims\bin\runserver.bat.

Accessing IMS Server diagnostic information

IMS Server diagnostic information can be obtain at the URL: https://imsserver/ims/ui/diagnostics. Note that you should be logged on to AccessAdmin first before navigating to this page.

It contains the list of SOAP services, IMS configuration information, test facilities for IMS Connectors, as well as descriptions of event and result codes.

Locating IMS Server's keystore

Encentuate IMS Server's keystore is in `%IMS_BASE%\ims\certs\keystore\ssl_keystore`.

Operations-related problems

Trusted certificate could not be found

If you encounter the following message,

```
javax.net.ssl.SSLHandshakeException:
java.security.cert.CertificateException: Couldn't find trusted
certificate
```

it is because the Encentuate IAM Authentication Bridge, Encentuate IAM Application Connector or command line tool (CLT) tried to connect to a remote server using SSL and failed because it was not configured to trust that server's certificate.

To trust the server's certificate, import the certificate or one of its issuers in the trust chain to the Authentication Bridge's, Application Connector's or CLT's keystore.

The Authentication Bridge's keystore is stated in the configuration file (`authBridge.xml`). The location of the file depends on what application the Authentication Bridge runs on. However, for a servlet application the files can be found in `/WEB-INF/`directory.

The Application Connector runs within Encentuate IMS Server and uses the Encentuate IMS Server’s keystore, which is in `%IMS_BASE%\ims\certs\keystore\ssl_keystore`.

The CLT's keystore is stated in the command line as a Java system property. For example, –`Djavax.net.ssl.security.trustStore=<filename>`. Typically this is set in the common setup file for the CLT which is `incSetupEnv.csh`.

CA certificate does not include basic constraints extension

If you encounter the following message,

```
javax.net.ssl.SSLHandshakeException:
java.security.cert.CertificateException: CA
certificate does not include basic constraints
extension
```

it is because one or more certificates in the chain of trust may be invalid. Check the certificates to ensure they are valid and have not expired, or that the validity period does not start on a future date.

If you find a certificate that is invalid, ask the Administrator to re-issue the certificate. This may require importing the certificate again. Alternatively import the actual trusted certificate that the server is using (versus the issuer’s certificate).

IMS Server unable to issue certificate for an application

It is a known bug that subject fields of IMS certificates can not contain the “_” character. This may cause problems at deployments that use certificate authentication for applications.

The result is that IMS Server cannot issue SCR or CAPI certificates for an authentication service with ID that contains the “_” character. The workaround is to remove all “_” characters from the IDs of authentication services that use certificate authentication.

Unable to access IMS Configuration Utility after IP address is changed

If the IP address of the IMS Server is changed, the IMS Configuration Utility becomes inaccessible from http://imsservername:8080/ unless the new IP address is included in the RemoteAddrValve configuration key of the <IMS Installation Folder>\conf\server.xml file. Restart the IMS Server after this configuration key is modified.

Alternatively, if you do not want to change the configuration key, you can still access the IMS Configuration Utility from http://localhost:8080/.

IMS Server database housekeeping problems

For normal database backup operations, the IMS database user only needs to have backup permissions on the IMS database. However, if the Housekeeping RDB System Backup Flag is set to true, the IMS database user must have administrative privileges, otherwise the following exception will appear in the IMS Server standard error logs:

java.sql.SQLException: [Microsoft][SQLServer 2000 Driver for JDBC][SQLServer]BACKUP DATABASE permission denied in database 'master'.

If cleanupRdbLogs is enabled (such as log table pruning), a “logs” directory should exist in the <IMS Installation Folder>\bin directory, otherwise the following exception will appear in the IMS Server standard error logs:

java.io.FileNotFoundException: logs\rdbLogCleanup.log (The system cannot find the path specified)

Unable to log on to AccessAdmin

If a user is unable to log on to AccessAdmin, check the following:

- Make sure that the user has the Administrator or Helpdesk role.
- If user is not using a USB Key, ensure that user’s Wallet has been cached.

AccessAdmin logon requires certificate authentication, which is only available for a cached Wallet or USB Key.

- Make sure that the machine wallet has been downloaded properly. See Machine Wallet download problem.

- Make sure that the DNS name of the IMS Server does not contain the "_" character. See IMS Server unable to issue certificate for an application.

- Make sure that the URL of AccessAdmin is exactly like how you specified it when you installed IMS. You can check the setting by accessing the IMS Server page and double-clicking the little lock icon to view the SSL certificate. The SSL certificate should list the exact hostname that you have to use.

- If you are using Windows 2003 and the homepage of Internet Explorer starts at something like "res://../hardAdmin.htm", the "Advanced Security Option" may have been enabled. You must go to the Add/remove programs menu from the Control Panel and choose to Add/remove Windows components. Look to remove the "Internet Explorer Enhanced Security

- Configuration, after which Internet Explorer's homepage should now be something like "res://../softAdmin.htm".

Machine Wallet download problem

When a machine starts up with a missing machine Wallet, AccessAgent will attempt to create the machine Wallet by downloading the latest policies and AccessProfiles from the current IMS Server. However, if IMS Server is not reachable, AccessAgent will use the policies and AccessProfiles specified in the following file: C:\Program Files\Encentuate\all_sync_data.xml.

To confirm whether the machine Wallet has been downloaded properly, you can run AccessStudio, load AccessProfiles from AccessAgent, and then click on sso_site_web_ims_admin under AccessProfiles. The machine Wallet is correct if the "@domain" field on the right panel is set to the IMS Server name. If the "@domain" field is "$hostname", the machine Wallet has not been downloaded properly.

If, for some reason, AccessAgent cannot download the policies and AccessProfiles from the IMS Server successfully despite multiple attempts at performing manual synchronization, you may want to edit the policies and AccessProfiles in the all_sync_data.xml file directly. Then perform the following operations to refresh the machine Wallet:

1. Log off AccessAgent (if logged on).

2. Stop the AccessAgent processes: AATray.exe, DataProvider.exe, and Sync.exe.

3. Stop the SOCIAccess service (net stop sociaccess).

4. Delete machine Wallet.

5. Restart machine.

In some deployments, workstations may only be able to connect to network after a user logs on to Windows. Since AccessAgent needs to download system data from IMS Server during the first boot-up after installation, it will fail to do so in such workstations. This would cause AccessAgent to be unusable on first boot-up.

A workaround is for the first user to bypass EnGINA and log on to Windows directly. After that, subsequent users should be able to log on normally through EnGINA. A better alternative is to include the IMS Server's latest all_sync_data.xml file in the installation package as follows:

1. Launch AccessStudio.

2. Click *Tools >> Backup System Data* from IMS to File.

3. Click Backup, and save it as all_sync_data.xml.

4. Place all_sync_data.xml in the Config folder of the AccessAgent installer package.

Logon user interface failed to load

If upon startup, the following error message appears:

```
User Interface Failure

The Logon User Interface DLL xxx.dll failed to load…..
```

either EnGINA has not been properly installed or the Winlogon GINA registry entry has not been set correctly after AccessAgent was uninstalled. Perform the following operations to resolve the issue:

1. Restart computer.

2. Go to Safe Mode by pressing F8 before Windows starts.

3. Log on as Administrator.

4. Modify the following Windows registry value: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]"GinaDLL"

5. If the value was **engina.dll**, EnGINA was probably not installed properly and could not load. Change the value to **msgina.dll**. The default Windows Logon prompt will be displayed on startup.

6. Should you desire to use EnGINA again after fixing the problem, change the value to **engina.dll**.

Active Directory

Search and get attributes do not work

Search refers to the search option (using Active Directory attributes) in *AccessAdmin >> Search Users >> New Search*. **Getattributes** refers to the user's attributes that cannot be edited when the search shows the profile of the user.

If the search and getattributes in AccessAdmin do not work, verify that the Active Directory connector is properly configured in the IMS Configuration Utility. The default connector should specify the Encentuate IAM Application Connector that is being used.

Search and getattributes functions match a user attribute retrieved from the Active Directory to a unique IMSID attribute present in Encentuate IMS Server's database. The Active Directory attribute is specified in the LDAP Active Directory User ID attribute and the IMSID attribute is specified in IMS attribute name—both in the IMS Configuration Utility.

The corresponding values of these attributes must be the same for Encentuate IMS Server to do the mapping correctly. In most deployments, the value for this attribute will be the same as the registration or bind attribute.

Automatic sign-on does not work properly for Microsoft GINA

For IMS Server versions between 3.1.1.6 and 3.1.7.1, the domain name is wrongly generated for the authentication service representing Windows credentials.

When you configure an enterprise directory for an Active Directory server, IMS Server automatically generates some authentication services, one for each Active Directory domain.

You can view the auto-generated authentication services on IMS Configuration Utility, by clicking **Authentication Services** in the left panel and select the authentication service from the drop down list.

For an authentication service representing an Active Directory domain, two domain names are included in the "Server locators to be used during injection": one is the DNS domain name (for example, "test.encentuate.com", while the other is the NETBIOS domain name (for example, "encentuate_test").

For automatic sign-on to be performed properly at Microsoft GINA, ensure that the NETBIOS domain should be the first one in the list.

Unable to return to EnGINA from Windows GINA

Users will not be able to return to EnGINA from Windows GINA by clicking the **Cancel** button if the following domain group policy is set to **Enabled**:

[Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options]

"Disable CTRL+ALT+DEL requirement for logon".

To fix this problem, it is necessary to set it to **Disabled** or **Not Defined**.

Anti-virus software interfering with AccessAgent or IMS Server

Some anti-virus software have been observed to interfere with AccessAgent or IMS Server, causing the following symptoms:

- AccessAgent (on user's PC, terminal server, or Citrix server) may become very slow.
- AccessAgent (on user's PC, terminal server, or Citrix server) may fail to start.
- Logon to AccessAgent (on terminal server or Citrix server) may fail intermittently.
- IMS Server may become very slow.

So far, the above problems have been observed at deployments that use McAfee anti-virus. The solution would be to put the frequently-changing Encentuate folders (**C:\Program Files\Encentuate\logs** for AccessAgent, and **C:\Encentuate** for IMS Server) in the anti-virus software's exclusion list. For McAfee, this can be done as follows:

1. Open the scanner's property pages.
2. On the Detection tab, under **What not to scan**, use the exclusions feature.
3. Click **Exclusions** to open the **Set Exclusions** dialog box.
4. Add files, folders, or drives or edit an item in the list.
5. To add an item, click **Add** to open the **Add Exclusion** Item dialog box.
6. Under **What to exclude**, select the desired folder using **By name/ location**.
7. Under **When to exclude**, specify all options.
8. Click **OK** to save these settings and return to the **Set Exclusions** dialog box.
9. Click **OK** to save these settings and return to the **Detection** tab.
10. Click **Apply** to save these settings.

ADSI connector

Unable to verify credentials

If you are configuring the ADSI Connector and are prompted that the credentials cannot be verified it is because the computer has not joined the domain.

MSDE

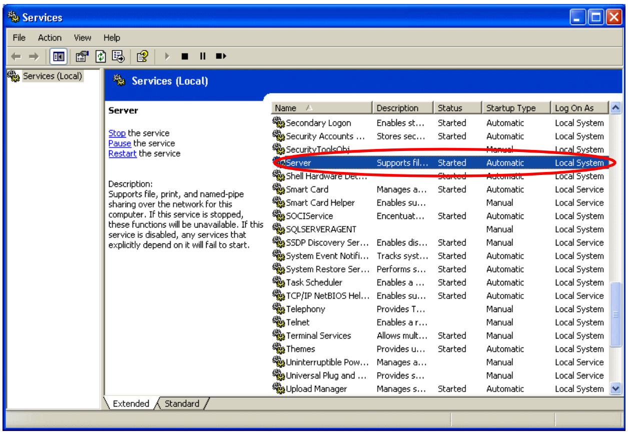
Problems installing MSDE

If you encounter the following problems it is an indication that your Microsoft SQL Desktop Edition (MSDE) installation was not successful:

- MSDE's installation progress bar goes backwards during installation.
- The installer unloads MSDE without any message.

Before you try again make sure of the following:

- You are logged on as an Administrator.
- Windows' server service is running and set to *automatic*.



Server

Stop the service
Pause the service
Restart the service

Description:
Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables st...	Started	Automatic	Local System
Security Accounts ...	Stores sec...	Started	Automatic	Local System
SecurityToolsObj			Manual	Local System
Server	Supports fil...	Started	Automatic	Local System
Shell Hardware Det...		Started	Automatic	Local System
Smart Card	Manages a...	Started	Automatic	Local Service
Smart Card Helper	Enables su...		Manual	Local Service
SOCIService	Encentuat...	Started	Automatic	Local System
SQLSERVERAGENT			Manual	Local System
SSDP Discovery Ser...	Enables dis...	Started	Manual	Local Service
System Event Notifi...	Tracks syst...	Started	Automatic	Local System
System Restore Ser...	Performs s...	Started	Automatic	Local System
Task Scheduler	Enables a ...	Started	Automatic	Local System
TCP/IP NetBIOS Hel...	Enables su...	Started	Automatic	Local Service
Telephony	Provides T...		Manual	Local System
Telnet	Enables a r...		Manual	Local System
Terminal Services	Allows mult...	Started	Manual	Local System
Themes	Provides u...	Started	Automatic	Local System
Uninterruptible Pow...	Manages a...		Manual	Local Service
Universal Plug and ...	Provides s...		Manual	Local Service
Upload Manager	Manages s...	Started	Automatic	Local System

Server Service

Unable to use port 1433

If an MSDE version earlier than Service Pack 3 is installed on Windows XP Service Pack 2, there may be no error during installation. However, due to some security vulnerability of the old version of MSDE, Windows disallows the SQL server to use port 1433. This results in failure to connect to the database during IMS Server installation.

If you check the Event Viewer, in Applications category, you would find some logs generated by SQL server, which indicate that port 1433 cannot be used because there is some vulnerability in the current version of MSDE.

To resolve this issue, apply MSDE 2000 Service Pack 3 (or newer), or just download the latest release of MSDE installer from Microsoft website.

SQL Server 2000

Failure to connect to named instance of SQL Server 2000 database

If you are upgrading from an IMS Server version earlier than 3.3.1.4, the upgrade may fail if the IMS database is a named instance of a SQL Server 2000 database.

If you encounter the following message:

There was a problem uploading all_storage_templates.xml.

this is because Microsoft's SQL Server 2000 JDBC driver used prior to IMS Server version 3.3.1.4 ignored the database port number field if a named instance is used. This prevents the IMS Server from connecting to the database.

In the SQL Server 2005 JDBC driver used in IMS Server version 3.3.1.4 and above, the port number field is not ignored and database connection would fail if the port number is wrong.

To fix this problem during an IMS Server upgrade, modify the IMS Server configuration file to correct the port number:

- Provide the correct port number in the following keys in the ims.xml file (found in **<IMS Installation Folder>\ims\config**): ds.ims.rdb.uri and ds.ims_log.rdb.uri.

  For example, if the correct port number is 1074, replace "jdbc:microsoft:sqlserver://serverName\instanceName:1433" with "jdbc:microsoft:sqlserver://serverName\instanceName:1074".

You can find the port number that the instance is running on by clicking on Start >> Programs >> Microsoft SQL Server >> Server Network Utility. Choose TCP/IP. Click **Properties**. *Right-click on database server and select* **Properties**.

- For a fresh IMS Server installation, make sure that the port number that you specify in the installation wizard is correct.

AccessAgent

Accessing AccessAgent logs

To troubleshoot AccessAgent problems, it is useful to take a look at the log files in **C:\Program Files\Encentuate\logs** folder.

XML files indicate communications with IMS Server and are useful for troubleshooting failure due to AccessAgent-IMS Server interaction.

AccessAgent.log logs internal AccessAgent processes and are useful for troubleshooting internal failure in AccessAgent.

aa_observer.log logs the observation of applications for automatic sign-on.

For installation problems, the AccessAgent installer logs can be found in C:\AAInstaller.log.

When reporting a bug, it is useful to include a zip file that contains the entire C:\Program Files\Encentuate\logs folder. Provide the approximate local times at which the events occurred.

If you cannot view or access the AccessAgent logs, it's possible that the logs have been hidden for security purposes. Be sure that the policy pid_log_obfuscation_enabled is set to No.

Increasing AccessAgent log level

It is useful to increase the log level so that more debugging information can be produced.

The log level is specified by the machine policy pid_log_level, which can be set through AccessAdmin.

Log level 3 is usually enough for most debugging purposes. If more detailed logs are required, the log level can be set to 4.

Synchronization with IMS Server

AccessAgent performs synchronization with the IMS Server periodically according to the frequency specified by pid_wallet_sync_mins. At times, it is useful to manually invoke the synchronization so that the latest policies or AccessProfiles can be downloaded. This is especially useful during troubleshooting or demos.

The AccessAgent right-click option for Synchronize with IMS can be enabled by setting the machine policy pid_wallet_manual_sync_enabled to 1, which can be set through AccessAdmin.

AccessAgent fails to install

If AccessAgent fails to install, check the following:

- Windows Scripting Host 5.6 and above should be installed.

- WMI needs to be functional. This can be verified by going into *Computer Management >> Services and Applications >> WMI Control*. Right-click on Properties and see if the message "Successfully Connected to: <local computer>" shows up. If it does not, AccessAgent will not install.

Installing ENGINA on Citrix servers

If AccessAgent 3.5 and below was previously installed without EnGINA, EnGINA will not be installed on subsequent installation of AccessAgent even if EnginaEnabled flag is set to 1 in **SetupHlp.ini**.

To fix the problem, remove the registry entry: [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\ActiveGinaAtUninstall] after uninstalling AccessAgent.

If AccessAgent was installed without EnGINA, and you decide to enable EnGINA later manually by setting the GinaDLL registry entry, reinstate the GinaDLL registry entry before uninstalling AccessAgent.

Otherwise, the GINA may not be set properly when another AccessAgent is installed.

Auto-admin logon using a domain account

AccessAgent is logged off if you are using an auto-admin account in a private desktop scenario.

Application does not behave properly after AccessAgent is installed

Some Microsoft DLLs are used by AccessAgent when observing applications. If the DLL versions are in conflict with those that are used by an application, the application may misbehave.

You can do the following to check if there may be DLL conflicts (also known as **DLL hell**):

- Launch command prompt (*Start* >> *Run* >> *cmd*).
- net stop obsservice
- Launch the application and see if it behaves correctly now.

If so, you can check the application folder to see if it is carrying any Microsoft DLLs, which are usually named ms*.dll (for example, **msvcr70.dll**, **msvcp70.dll**).

One possible fix for this problem is to use the DLL redirection configuration suggested by Microsoft: http://msdn2.microsoft.com/en-us/library/ms682600.aspx.

Another possible fix is to replace the DLL that is carried by the application with the DLL that is compatible with AccessAgent. However, that requires that the application is also compatible with the same DLL.

AccessAgent unable to connect to IMS Server

If AccessAgent is unable to connect to the IMS Server, it will not be able to perform certain operations, such as:

- Logging on to AccessAgent when there is no existing cached Wallet for the user.
- Changing of Encentuate or USB Key password.
- Registering a 2nd factor.
- User sign up.

The following situations could prevent AccessAgent from connecting to the IMS Server:

- Client machine is not on the network.
- Client machine has no network connectivity (or lost connectivity) to IMS Server. This could be due to an intervening firewall between the client machine and IMS Server, or due to some network configuration issues, such as DNS problems.
- Client machine has a personal firewall or anti-spyware that is blocking traffic from AccessAgent. To allow AccessAgent to contact IMS Server while computer is locked, the personal firewall or anti-spyware must also not be blocking traffic from winlogon.exe.
- Client machine does not have the IMS Server certificates installed on it, possibly because the client machine was offline during AccessAgent installation.
- AccessAgent registry settings are corrupted or mis-configured (for example, AccessAgent is pointing to the wrong IMS Server).

AccessAgent unable to download IMS Server certificate

If configured properly, the AccessAgent installer should download the IMS Server certificate to the client PC. However, this download may fail if the client PC is offline or the IMS Server is not available at that time. The server certificate can be downloaded after installation through any of the following methods:

1. *Click Start >> All Programs >> Encentuate AccessAgent >> Set IMS Server Location*

2. Run **C:\Program Files\Encentuate\SetupCertDlg.exe**.

AccessAgent does not display correct domain

For IMS Server version 2.x:

- When user logs on with password, AccessAgent shows, in the Domain field of the logon prompt, the display name of the authentication service specified by **pid_bind_auth_list**. To modify the displayed domain, use AccessStudio or IMS Configuration Utility to modify the display name of the appropriate authentication service.

For IMS Server version 3.x and above:

- The policy **pid_bind_edir_list** replaces **pid_bind_auth_list**. AccessAgent shows the domains specified in the enterprise directory listed in **pid_bind_edir_list**.

Unable to log on to cached Wallets

If AccessAgent can log on when IMS Server is online, but cannot log on to cached Wallets when IMS Server is offline, the cached Wallets may be corrupted. In such cases, it may be necessary to delete all cached Wallets and try logging on again.

Enable the AccessAgent right-click option for **Delete user Wallets** by setting the machine policy **pid_wallet_delete_enabled** to 1, which can be set through AccessAdmin.

The menu item is only available when no user is logged on to AccessAgent. Only user Wallets are deleted and not the machine Wallet.

If this feature is to be used on a Citrix or Terminal Server or a workstation with Local User Session Management (LUSM) enabled, make sure that only one desktop session is running while deleting the Wallets.

If multiple sessions are running, the behavior of AccessAgent in other sessions after deleting the Wallets is unpredictable.

Unable to log on to the Wallet after AccessAgent is freshly installed

If you are using a version of AccessAgent before 3.3.1.4, there is a bug that prevents users from logging on if the machine Wallet is bigger than 2MB. This can happen if there is a large number of AccessProfiles.

When attempting to log on, users will see the following “Cannot Log On” error prompt:

```
You do not have a Wallet stored on this computer.
However, you cannot download your Wallet from the IMS
Server because network connectivity is currently
unavailable. Please try again later.
```

- Upgrade to AccessAgent version 3.3.1.4 or above.
- Reduce the number of AccessProfiles such that the machine Wallet is not more than 2MB in size.

Note that the inability to log on may also be due to any of the problems listed in AccessAgent unable to connect to IMS Server.

APPENDICES

Appendices

Refer to the following appendices for more useful information on setting up Encentuate IAM for your organization:

- Appendix A: Installing The IMS Database
- Appendix B: Definitions of policies
- Appendix C: Using The IMS Configuration Utility

Installing The IMS Database

Encentuate recommends Microsoft SQL Server 2000 Desktop, Standard or Enterprise Edition with Service Pack 3. A copy of MSDE with Service Pack 3 is available on the IMS Server installation CD.

The database can be installed on the same computer where you will be installing IMS Server or on a remote computer. If the database is located on a remote computer, MS SQL Server must also be installed on the computer where you are installing the IMS Server.

Should the IMS database and IMS Server be running on different machines, it is recommended that the system clocks be synchronized. This can be achieved through the use of the time synchronization feature of Microsoft Windows that is based on Network Time Protocol (NTP). More information on the time synchronization feature of Windows can be found at:

- Windows 2000: http://support.microsoft.com/kb/224799
- Windows XP: http://support.microsoft.com/kb/307897
- Windows Server: http://support.microsoft.com/kb/816042

You must know the Server Administrator (Sa) account name and password. The default Sa is `sa` and the password is `admin`.

Installation pre-requisites

For Microsoft SQL Server 2000

- Microsoft SQL Server 2000 (Standard, Enterprise, or Desktop Edition) with Service Pack 3.
  - SQL Server Authentication should be enabled. This can be done by using the SQL Enterprise Manager: *Right-click DB Server >> Click the* **Security** *tab >> Choose* SQL Server and Windows *authentication.*

- The SQL Server should have TCP connections, SQL Server Authentication enabled. This can be done using the SQL Enterprise Manager: *Right-click DB Server >> General tab >> Network Configuration button >> Enable TCP/IP and Named Pipes*.

- If a named instance is used, the name of the instance and the port that the instance is running on should be known. You can check the port number by using the SQL Enterprise Manager: *Right-click DB Server/instance >> General tab >> Network Configuration button >> Select TCP/IP >> Click Properties*.

- Disable all default connection options. This can be done by using the SQL Enterprise Manager: *Right-click DB Server >> Connections tab >> Uncheck all Default connection options*.

- Administrator (SA) account and password for Microsoft SQL Server.

- For Administrator-created database, note that database collation should be SQL_Latin1_General_CP1_CS_AS.

- For Administrator-created database user, note that the user should have public, db_owner rights for the created database. The user should not be a DB Administrator account.

For Microsoft SQL Server 2005

- Microsoft SQL Server 2005 (Standard, Enterprise, or Express Edition) with Service Pack 1.

  - SQL Server Authentication should be enabled. This can be done by using the SQL Server Management Studio: *Right-click DB Server >> Click on Security on the left panel >> Choose SQL Server and Windows Authentication mode*.

  - The SQL Server should have TCP connections, SQL Server Authentication enabled. This can be done using the SQL Server Configuration Manager: *Click on SQL Server Network Configuration >> Protocols >> Double-click TCP/IP >> Protocol tab > Set Enabled to Yes*.

  - Choose a static port for TCP connections. This can be done using the SQL Server Configuration Manager: *Click on SQL Server Network Configuration >> Protocols >> Double-click TCP/IP >> IP Addresses tab >> Blank out all TCP Dynamic Ports >> Fill in all TCP Ports with 1433/any available static port.*

  - If a named instance is used, the name of the instance should be known.

  - Disable all default connection options. This can be done by using the SQL Server Management Studio: *Right-click DB Server >> Click on Connections in the left panel >> Uncheck all Default connection options*.

- Administrator (SA) account and password for Microsoft SQL Server.

- For Administrator-created database, note that database collation should be SQL_Latin1_General_CP1_CS_AS.

- For Administrator-created database user, note that the user should have public, db_owner rights for the created database. The user should not be a DB Administrator account

For Oracle

You must have the following:

- Oracle 9i/10g Database with an instance created for the Encentuate IMS Server.

- Administrator (DBA) account and password for this instance, to be used by the Encentuate IMS Server.

Installing MSDE

To install a new instance of Desktop Engine:

1. Open a command prompt window.

2. From the command prompt, use the **cd** command to navigate to the folder containing the MSDE 2000 setup:

   ```
   cd c:\MSDE2000AFolder
   ```

   Where *c:\MSDE2000AFolder* is the path of the folder where you extracted the MSDE 2000 setup files.

3. Execute the following command to install a default instance configured to use Mixed Mode:

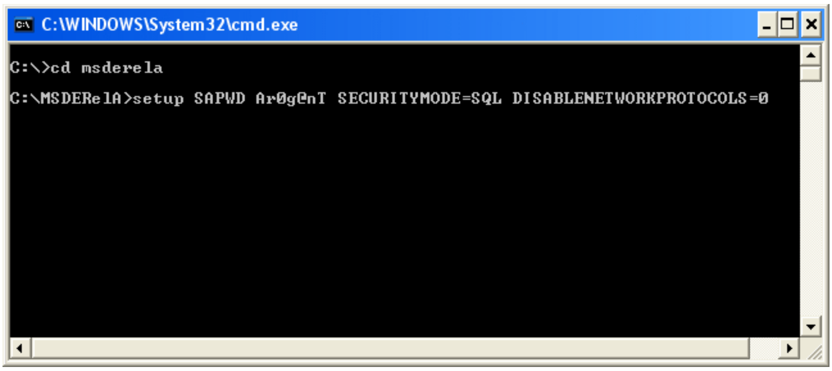
   ```
   setup SAPWD="AStrongSAPwd" SECURITYMODE=SQL
   DISABLENETWORKPROTOCOLS=0
   ```

   Where:

   AStrongSAPwd is a strong password to be assigned to the **sa** logon.

SECURITYMODE=SQL specifies that the instance be installed in Mixed Mode, where the instance supports both Windows Authentication and SQL Authentication logins.

DISABLENETWORKPROTOCOLS=0 enables network support for an instance of MSDE 2000



```
C:\>cd msderela

C:\MSDERelA>setup SAPWD Ar0g@nT SECURITYMODE=SQL DISABLENETWORKPROTOCOLS=0
```

Command Prompt Commands

The installation will start. Once installation is complete you should see the MS SQL Server icon in the notification area.

Using an Oracle database

Currently Oracle 9i /10g database are supported. If you will be using an Oracle database with the IMS Server, you must configure a few things which are discussed in this section. This section does not cover installation of Oracle database or client. It is assumed an Oracle database is already installed.

To set up an Oracle database with the IMS Server:

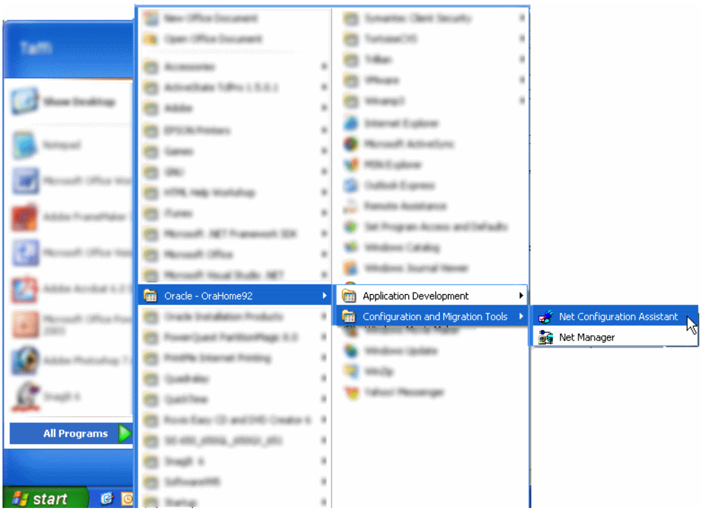
1. Create an Oracle 9i/10g database (instance) for the Encentuate IMS Server.
2. Create an Administrator (DBA) account and password for the instance.
3. Install Oracle client on the local computer where you are installing IMS Server.
4. Define a net service name for the Oracle 9i/10g instance on the local computer where you are installing IMS Server.

The nest section provides step-by-step instructions on setting up an Oracle database.

Creating a database

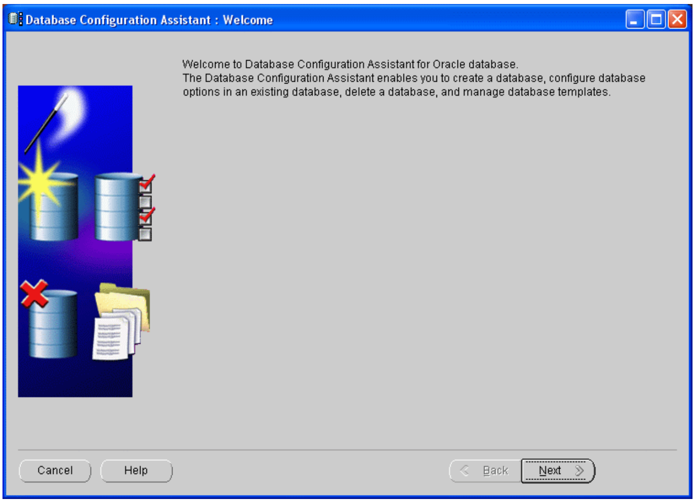
To create a database in Oracle 9i/10g for the IMS Server:

1. Access the **Net Configuration Assistant** from *Start >> Programs >> Oracle-OraHome93 >> Configuration and Migration Tools*.



Net Configuration Assistant

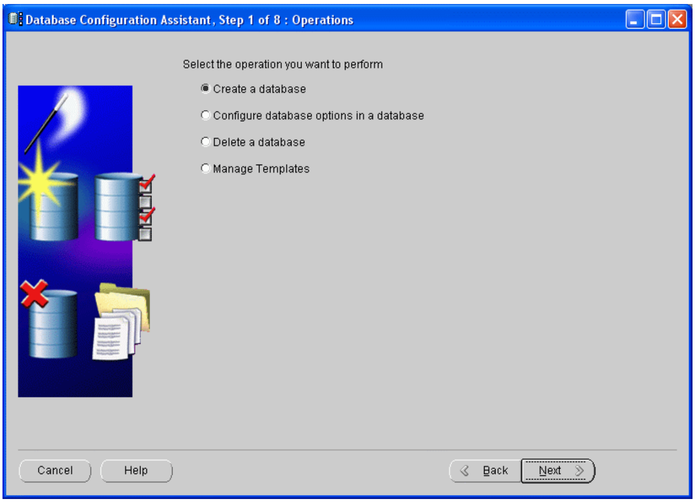
2. Click **Next**.



Welcome to Database Configuration Assistant for Oracle database.
The Database Configuration Assistant enables you to create a database, configure database options in an existing database, delete a database, and manage database templates.

General Information

3. Choose to **create a database**.



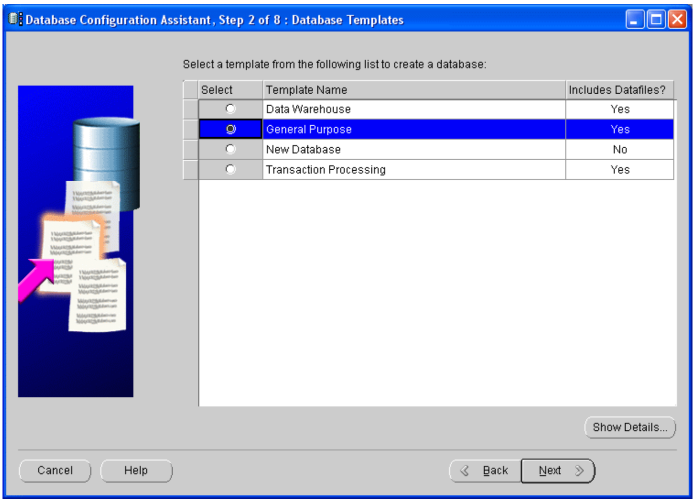
Database Configuration Assistant, Step 1 of 8 : Operations

Select the operation you want to perform

- ● Create a database
- ○ Configure database options in a database
- ○ Delete a database
- ○ Manage Templates

Create a Database

❹ Select **General Purpose** as the template for the database.



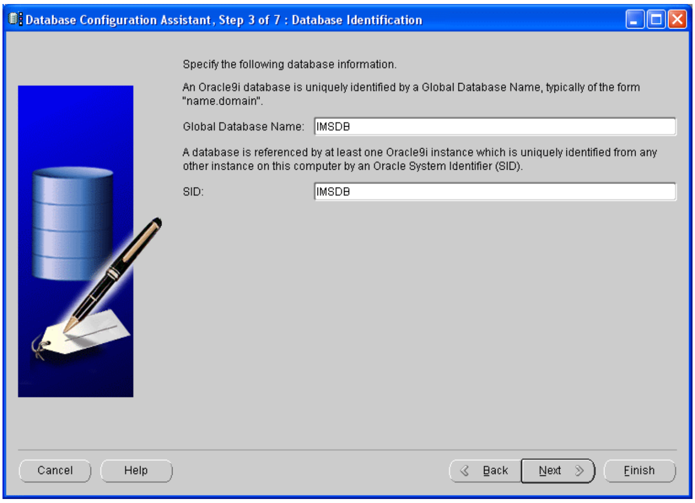
Database Configuration Assistant, Step 2 of 8 : Database Templates

Select a template from the following list to create a database:

Select	Template Name	Includes Datafiles?
○	Data Warehouse	Yes
●	General Purpose	Yes
○	New Database	No
○	Transaction Processing	Yes

General Purpose

❺ Specify a database name. The name you specify for the database will also be the Oracle System Identifier (SID) by default. It is highly recommended that the global database name and SID be identical. You should take note of the SID as you will need to enter it later.



Database Configuration Assistant, Step 3 of 7 : Database Identification

Specify the following database information.

An Oracle9i database is uniquely identified by a Global Database Name, typically of the form "name.domain".

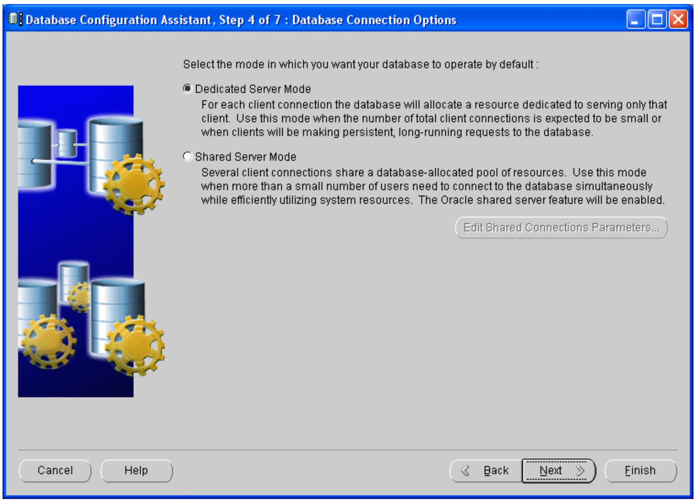
Global Database Name: IMSDB

A database is referenced by at least one Oracle9i instance which is uniquely identified from any other instance on this computer by an Oracle System Identifier (SID).

SID: IMSDB

Database Name and SID

❻ Select **Dedicated Server Mode** for your database.



Database Configuration Assistant, Step 4 of 7 : Database Connection Options

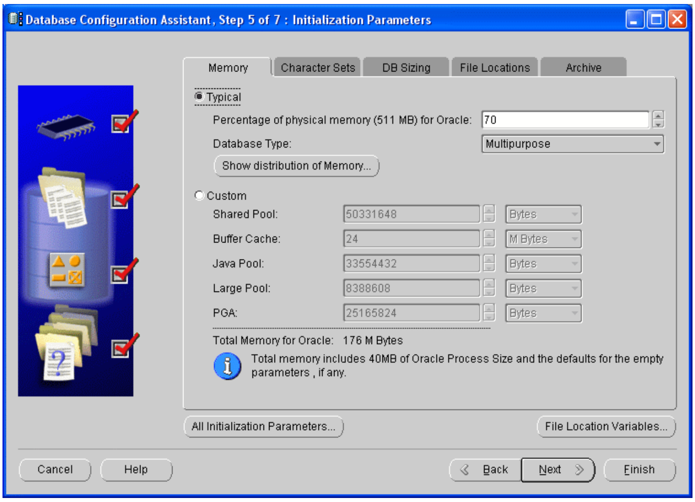
Select the mode in which you want your database to operate by default :

● Dedicated Server Mode
For each client connection the database will allocate a resource dedicated to serving only that client. Use this mode when the number of total client connections is expected to be small or when clients will be making persistent, long-running requests to the database.

○ Shared Server Mode
Several client connections share a database-allocated pool of resources. Use this mode when more than a small number of users need to connect to the database simultaneously while efficiently utilizing system resources. The Oracle shared server feature will be enabled.

Dedicated Server Mode

❼ Choose **Typical** for the initialization parameters. Retain the current settings.


Memory
Character Sets
DB Sizing
File Locations
Archive
Show distribution of Memory...
All Initialization Parameters...
File Location Variables...
Cancel
Help
Back
Next
Finish

Database Configuration Assistant, Step 5 of 7 : Initialization Parameters

● Typical

Percentage of physical memory (511 MB) for Oracle: 70

Database Type: Multipurpose

○ Custom

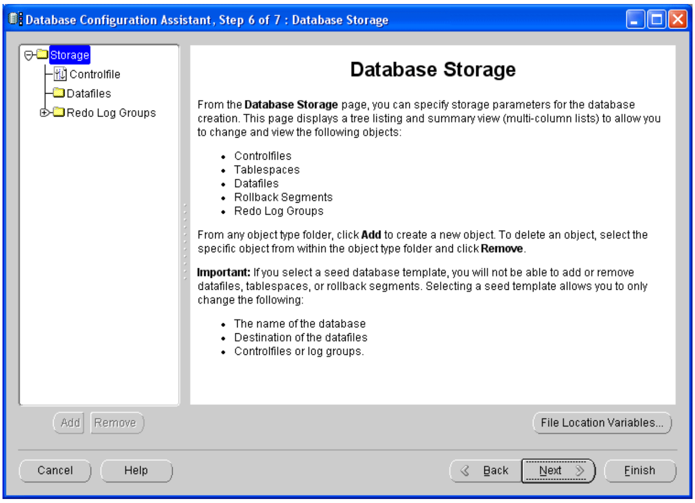
Shared Pool:	50331648	Bytes
Buffer Cache:	24	M Bytes
Java Pool:	33554432	Bytes
Large Pool:	8388608	Bytes
PGA:	25165824	Bytes

Total Memory for Oracle: 176 M Bytes

Total memory includes 40MB of Oracle Process Size and the defaults for the empty parameters , if any.

Typical settings

❽ Click **Next**.



Database Configuration Assistant, Step 6 of 7 : Database Storage

Database Storage

From the **Database Storage** page, you can specify storage parameters for the database creation. This page displays a tree listing and summary view (multi-column lists) to allow you to change and view the following objects:

- Controlfiles
- Tablespaces
- Datafiles
- Rollback Segments
- Redo Log Groups

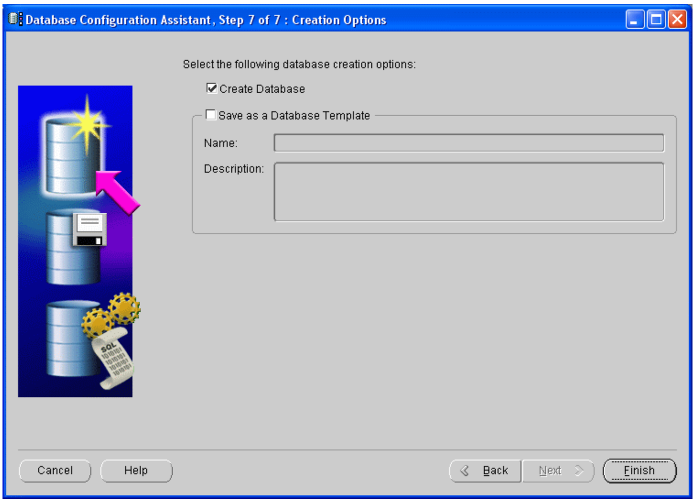
From any object type folder, click **Add** to create a new object. To delete an object, select the specific object from within the object type folder and click **Remove**.

Important: If you select a seed database template, you will not be able to add or remove datafiles, tablespaces, or rollback segments. Selecting a seed template allows you to only change the following:

- The name of the database
- Destination of the datafiles
- Controlfiles or log groups.

Database Storage Information

❾ Select **Create Database**.


Database Configuration Assistant, Step 7 of 7 : Creation Options
Cancel
Help
Back
Next
Finish

Select the following database creation options:

☑ Create Database

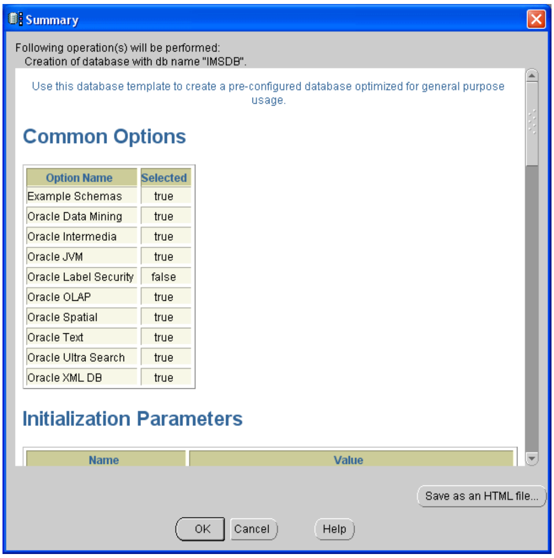
□ Save as a Database Template

Name:

Description:

Create Database

⑩ The next screen will show you the summary of the options you have selected. Click OK to continue.



Following operation(s) will be performed:
Creation of database with db name "IMSDB".

Use this database template to create a pre-configured database optimized for general purpose usage.

Common Options

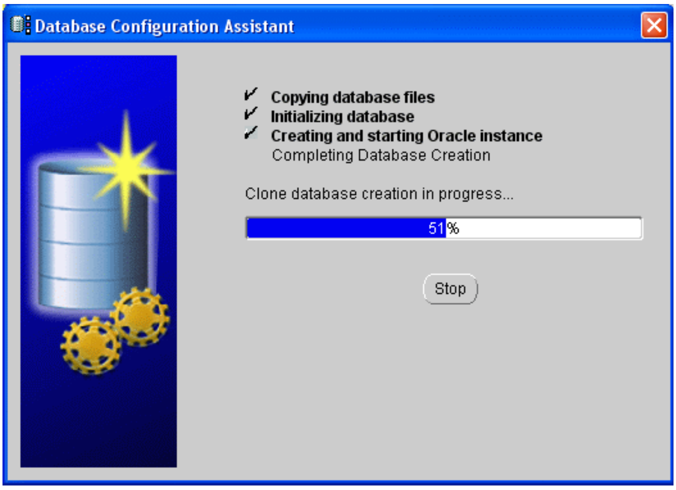
Option Name	Selected
Example Schemas	true
Oracle Data Mining	true
Oracle Intermedia	true
Oracle JVM	true
Oracle Label Security	false
Oracle OLAP	true
Oracle Spatial	true
Oracle Text	true
Oracle Ultra Search	true
Oracle XML DB	true

Initialization Parameters

Name	Value

Summary

The database creation will begin.



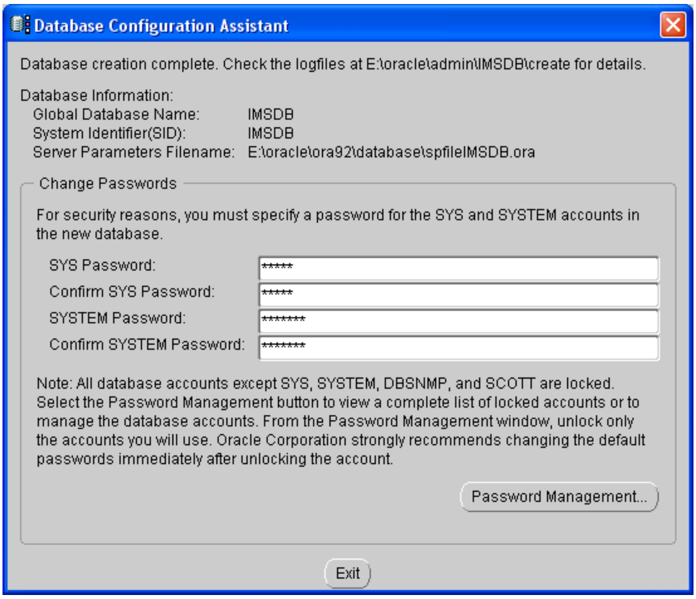
✓ Copying database files
✓ Initializing database
✓ Creating and starting Oracle instance
Completing Database Creation

Clone database creation in progress...

51%

Database Creation

⓫ Once the database creation is complete, you must specify new passwords for the *Sys* and *System* accounts.



Database creation complete. Check the logfiles at E:\oracle\admin\IMSDB\create for details.

Database Information:
Global Database Name: IMSDB
System Identifier(SID): IMSDB
Server Parameters Filename: E:\oracle\ora92\database\spfileIMSDB.ora

Change Passwords

For security reasons, you must specify a password for the SYS and SYSTEM accounts in the new database.

SYS Password: *****
Confirm SYS Password: *****
SYSTEM Password: *******
Confirm SYSTEM Password: *******

Note: All database accounts except SYS, SYSTEM, DBSNMP, and SCOTT are locked. Select the Password Management button to view a complete list of locked accounts or to manage the database accounts. From the Password Management window, unlock only the accounts you will use. Oracle Corporation strongly recommends changing the default passwords immediately after unlocking the account.

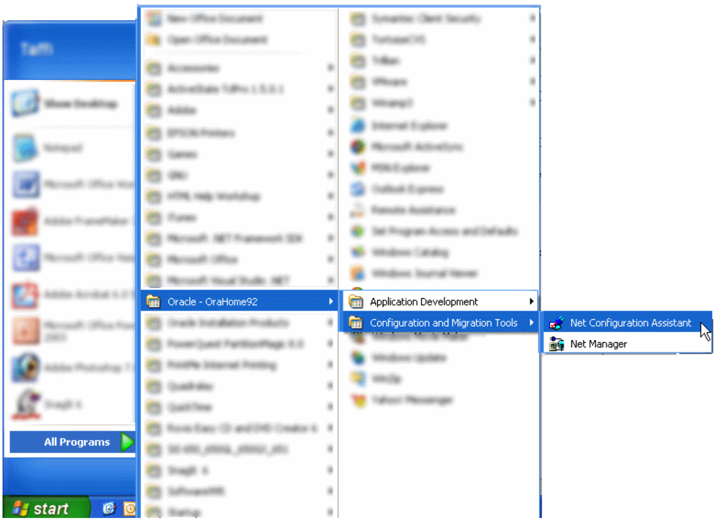
Database Creation

Creating a service name

You must create a service name for the Oracle 9i database which the IMS Server will connect to. Prior to this, you must install Oracle Client on the computer where you are installing the IMS Server.

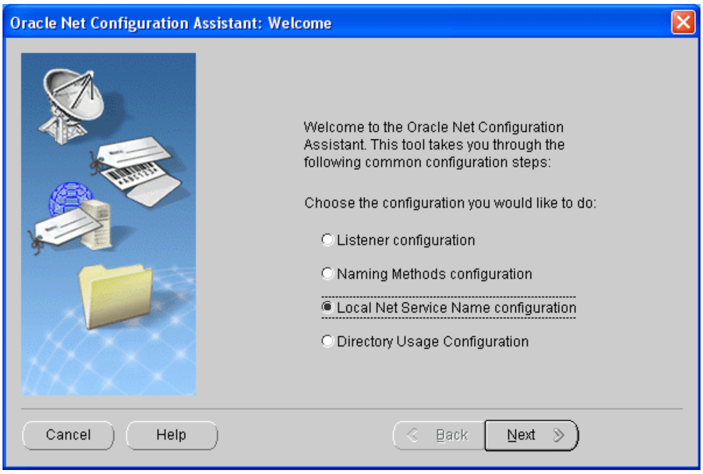
To create a service name:

❶ Access **Net Configuration Assistant** from *Start >> Programs >> Oracle - OraHome92 >> Configuration and Migration Tools*.



Net Configuration Assistant

❷ Choose **Local Net Service Name configuration**.



Oracle Net Configuration Assistant: Welcome

Welcome to the Oracle Net Configuration Assistant. This tool takes you through the following common configuration steps:

Choose the configuration you would like to do:

○ Listener configuration

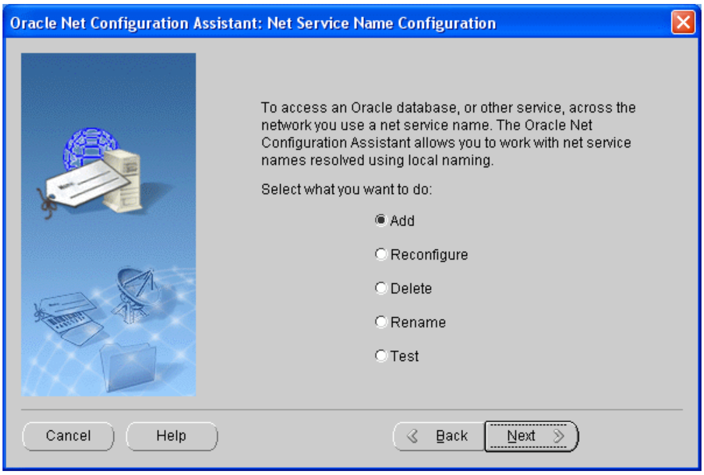
○ Naming Methods configuration

● Local Net Service Name configuration

○ Directory Usage Configuration

Local Net Service Name Configuration

❸ Select **Add**.



Oracle Net Configuration Assistant: Net Service Name Configuration

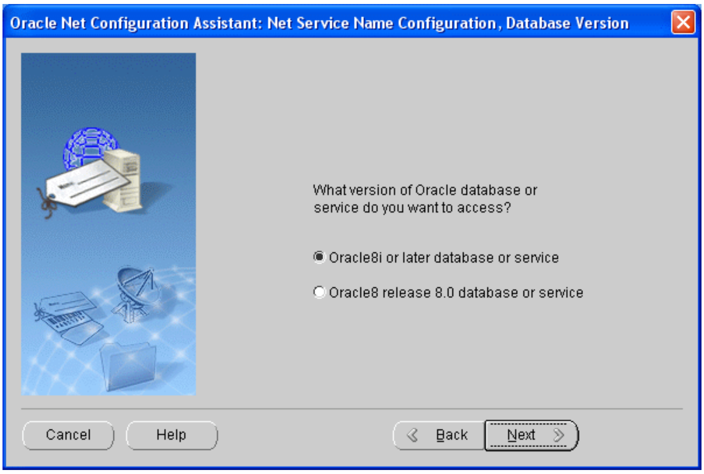
To access an Oracle database, or other service, across the network you use a net service name. The Oracle Net Configuration Assistant allows you to work with net service names resolved using local naming.

Select what you want to do:

- ● Add
- ○ Reconfigure
- ○ Delete
- ○ Rename
- ○ Test

Add

❹ Specify **Oracle 8i or later database or service**.



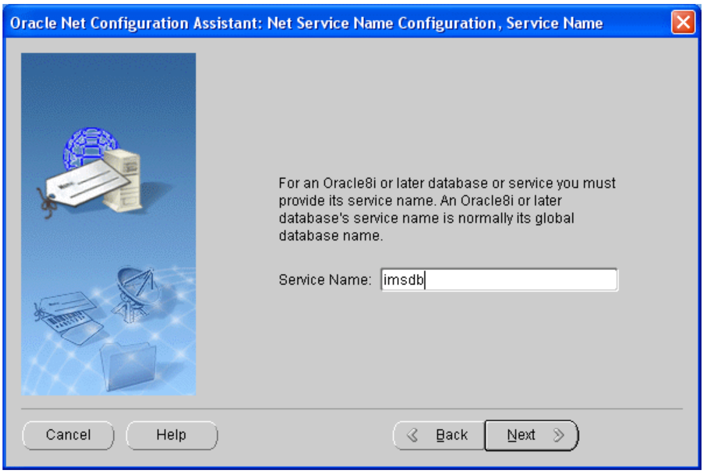
Oracle Net Configuration Assistant: Net Service Name Configuration, Database Version

What version of Oracle database or service do you want to access?

- ● Oracle8i or later database or service
- ○ Oracle8 release 8.0 database or service

Specify Version of Oracle

❺ Specify a service name.

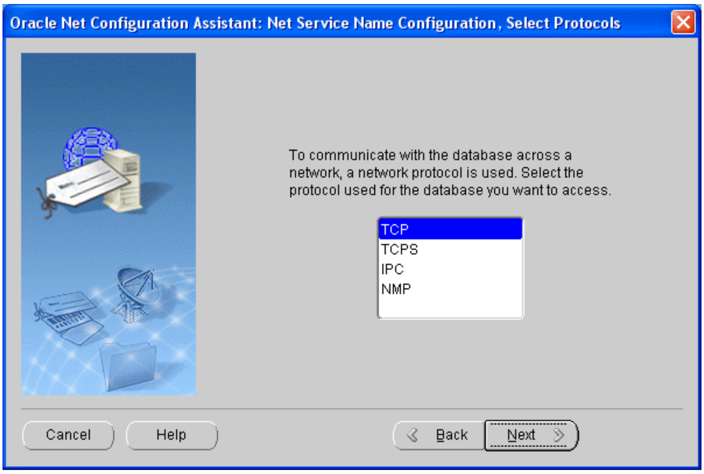

Oracle Net Configuration Assistant: Net Service Name Configuration, Service Name

For an Oracle8i or later database or service you must provide its service name. An Oracle8i or later database's service name is normally its global database name.

Service Name: imsdb

Specify a Service Name

❻ Choose TCP as the protocol.

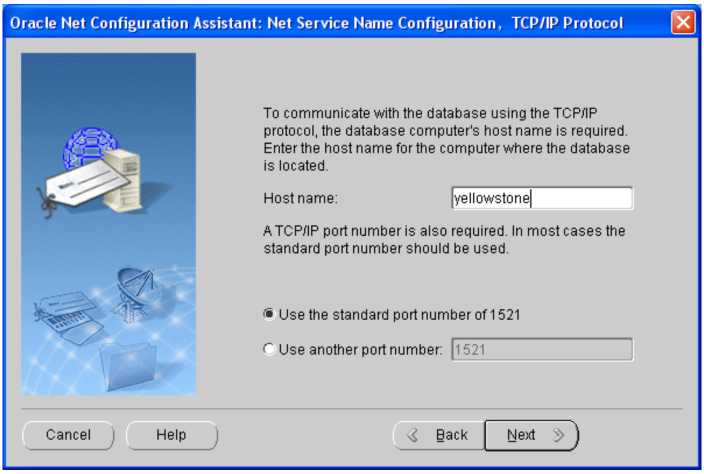

Oracle Net Configuration Assistant: Net Service Name Configuration, Select Protocols

To communicate with the database across a network, a network protocol is used. Select the protocol used for the database you want to access.

TCP (selected)

Choose Protocol

❼ Specify the host name of the computer where the database is located. Use the standard port number of 1521.



Oracle Net Configuration Assistant: Net Service Name Configuration, TCP/IP Protocol

To communicate with the database using the TCP/IP protocol, the database computer's host name is required. Enter the host name for the computer where the database is located.

Host name: yellowstone

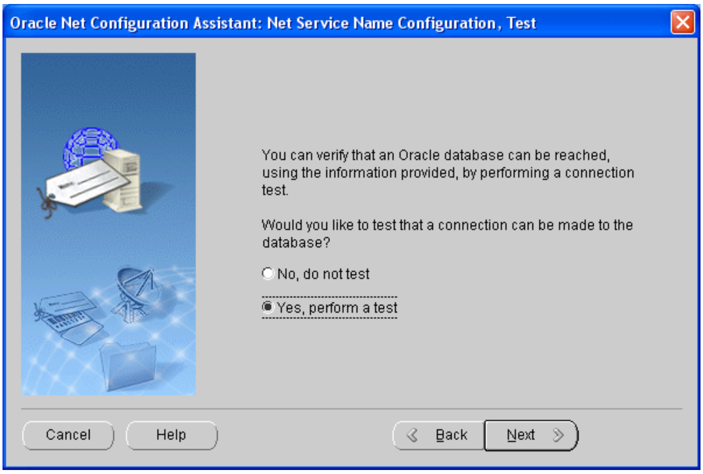
A TCP/IP port number is also required. In most cases the standard port number should be used.

● Use the standard port number of 1521

○ Use another port number: 1521

Hostname and Port Number

❽ Choose to perform a test.



Oracle Net Configuration Assistant: Net Service Name Configuration, Test

You can verify that an Oracle database can be reached, using the information provided, by performing a connection test.

Would you like to test that a connection can be made to the database?

○ No, do not test

● Yes, perform a test

Perform a Test

If the test fails, check to make sure a valid user name and password (that can connect to the database) is specified. For example, you can specify the DBA account created for the IMS Server or the default Oracle accounts (Sys, System or Scott).

An alternative way of defining the net service name for the Oracle 9i instance to be used on the local computer where you are installing the IMS Server, is to edit the file *tnsnames.ora* which can be found in *\ora92\network\admin*. Here *ora92* is the ORACLE_HOME directory created by the Oracle Client installation.

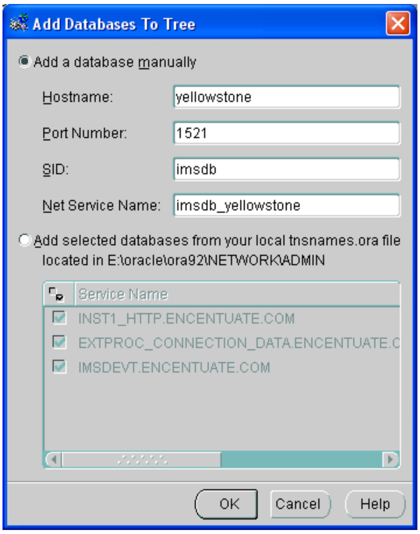
Using Oracle Enterprise Manager

Following are instructions on how to add a database to the Enterprise Manager so that it can be managed.

To add a database to the Enterprise Manager:

❶ Access the Oracle Enterprise Manager by going to *Start >> Programs >> Oracle – OraHome92 >>Enterprise Manager Console*.

❷ Select to **Add a database manually.** Specify the **host name, port number** and **SID** (the SID is created when the database is created).



● Add a database manually

Hostname: yellowstone

Port Number: 1521

SID: imsdb

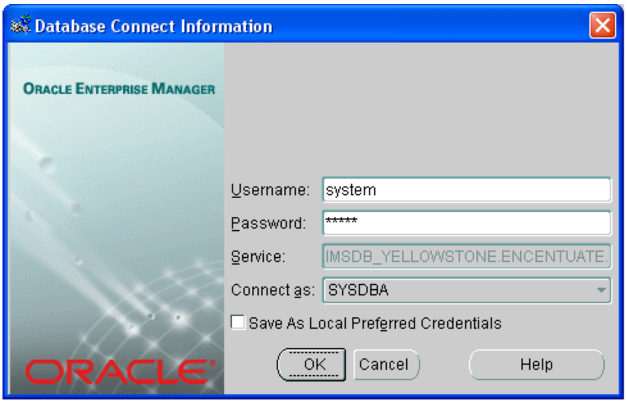
Net Service Name: imsdb_yellowstone

○ Add selected databases from your local tnsnames.ora file located in E:\oracle\ora92\NETWORK\ADMIN

Service Name
☑ INST1_HTTP.ENCENTUATE.COM
☑ EXTPROC_CONNECTION_DATA.ENCENTUATE.C
☑ IMSDEVT.ENCENTUATE.COM

Add a Database

❷ Specify the user name and password.



Username: system

Password: *****

Service: IMSDB_YELLOWSTONE.ENCENTUATE.

Connect as: SYSDBA

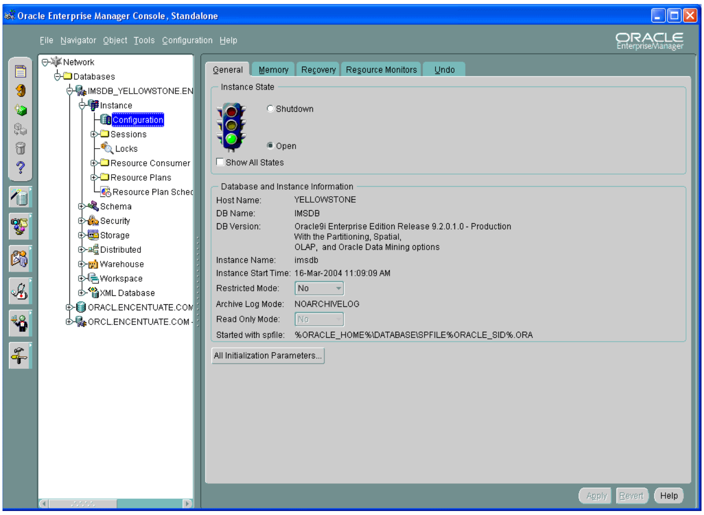
□ Save As Local Preferred Credentials

User Name and Password

Creating the user using Enterprise Manager

To create user using Enterprise Manager:

❶ Select the database you have created. Click **Instance** then **Configuration**.



Instance State

○ Shutdown

● Open

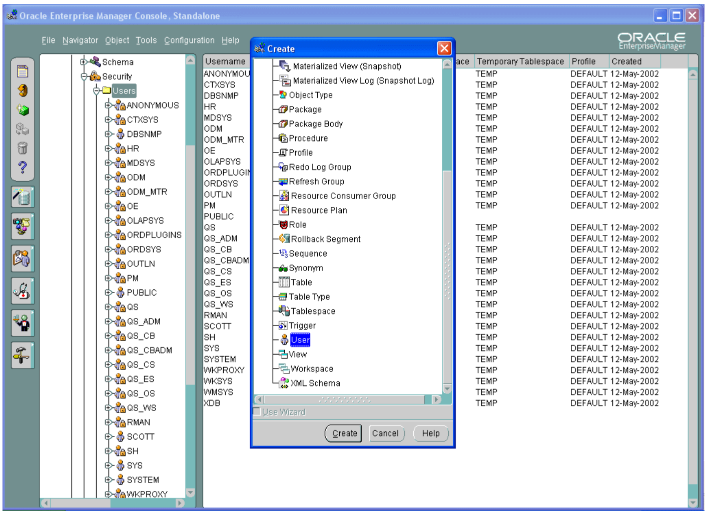
□ Show All States

Database and Instance Information

Host Name: YELLOWSTONE
DB Name: IMSDB
DB Version: Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production
With the Partitioning, Spatial,
OLAP, and Oracle Data Mining options
Instance Name: imsdb
Instance Start Time: 16-Mar-2004 11:09:09 AM
Restricted Mode: No
Archive Log Mode: NOARCHIVELOG
Read Only Mode: No
Started with spfile: %ORACLE_HOME%\DATABASE\SPFILE%ORACLE_SID%.ORA

Specify Name

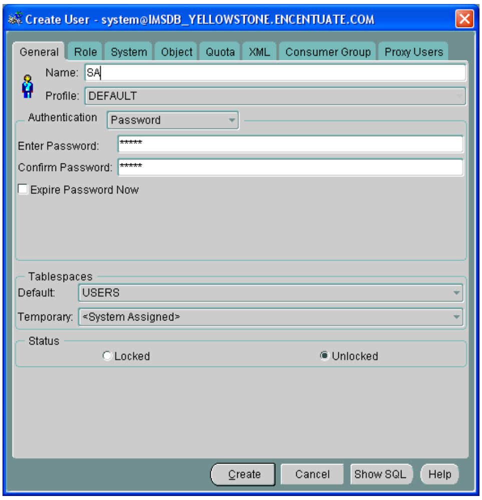
❷ Click **Security** and then **Users**. Choose to create a new user. When the Create dialog box comes, choose to create the user.



Username	ace	Temporary Tablespace	Profile	Created
ANONYMOU		TEMP	DEFAULT	12-May-2002
CTXSYS		TEMP	DEFAULT	12-May-2002
DBSNMP		TEMP	DEFAULT	12-May-2002
HR		TEMP	DEFAULT	12-May-2002
MDSYS		TEMP	DEFAULT	12-May-2002
ODM		TEMP	DEFAULT	12-May-2002
ODM_MTR		TEMP	DEFAULT	12-May-2002
OE		TEMP	DEFAULT	12-May-2002
OLAPSYS		TEMP	DEFAULT	12-May-2002
ORDPLUGII		TEMP	DEFAULT	12-May-2002
ORDSYS		TEMP	DEFAULT	12-May-2002
OUTLN		TEMP	DEFAULT	12-May-2002
PM		TEMP	DEFAULT	12-May-2002
PUBLIC				
QS		TEMP	DEFAULT	12-May-2002
QS_ADM		TEMP	DEFAULT	12-May-2002
QS_CB		TEMP	DEFAULT	12-May-2002
QS_CBADM		TEMP	DEFAULT	12-May-2002
QS_CS		TEMP	DEFAULT	12-May-2002
QS_ES		TEMP	DEFAULT	12-May-2002
QS_OS		TEMP	DEFAULT	12-May-2002
QS_WS		TEMP	DEFAULT	12-May-2002
RMAN		TEMP	DEFAULT	12-May-2002
SCOTT		TEMP	DEFAULT	12-May-2002
SH		TEMP	DEFAULT	12-May-2002
SYS		TEMP	DEFAULT	12-May-2002
SYSTEM		TEMP	DEFAULT	12-May-2002
WKPROXY		TEMP	DEFAULT	12-May-2002
WKSYS		TEMP	DEFAULT	12-May-2002
WMSYS		TEMP	DEFAULT	12-May-2002
XDB		TEMP	DEFAULT	12-May-2002

Choose to Create a New User

❸ In the **General** tab, specify the name and enter the corresponding password for it.



Create User - system@IMSDB_YELLOWSTONE.ENCENTUATE.COM

Name: SA

Profile: DEFAULT

Authentication: Password

Enter Password: *****

Confirm Password: *****

□ Expire Password Now

Tablespaces

Default: USERS

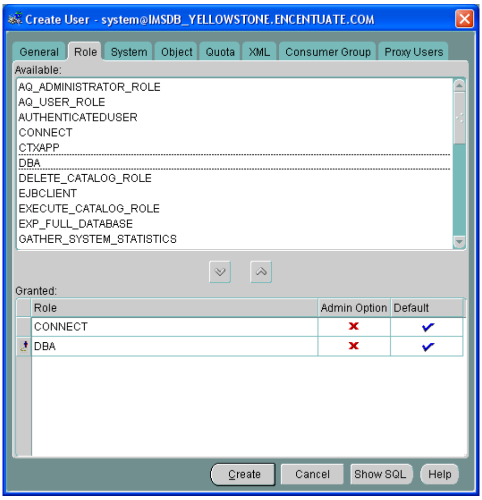
Temporary: <System Assigned>

Status

○ Locked ● Unlocked

Specify Name

❹ Click the **Role** tab and select one or more roles for the user. For example you can choose **DBA** for the *sa user* and CONNECT and RESOURCE for the *ims* user. Use the down arrow to add the roles.



Create User - system@IMSDB_YELLOWSTONE.ENCENTUATE.COM

Available:

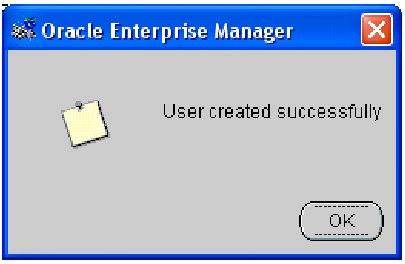
AQ_ADMINISTRATOR_ROLE
AQ_USER_ROLE
AUTHENTICATEDUSER
CONNECT
CTXAPP
DBA
DELETE_CATALOG_ROLE
EJBCLIENT
EXECUTE_CATALOG_ROLE
EXP_FULL_DATABASE
GATHER_SYSTEM_STATISTICS

Granted:

Role	Admin Option	Default
CONNECT	✗	✓
DBA	✗	✓

Add Role

❺ Click **Create** and the user will be created.



Oracle Enterprise Manager

User created successfully

User Created

Definitions of policies

Policies can be modified only by Helpdesk officers and Administrators, because these policies affect the behavior of the whole system and should only be modified when it is absolutely necessary. These policies should be set at deployment and followed through.

Changes to these policies are propagated to clients the next time AccessAgent synchronizes with the IMS Server.

Legend

Attribute	Description
Policy ID	Unique identifier of the policy.
Description	Description of the policy, including a list of the possible behaviors specified by the policy. The product version that implements this policy is also indicated.
Registry	The entry in the Windows Registry (for Machine policies) or the IMS (for System, User, and Machine policies): ■ [DO] is [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\DeploymentOptions] ■ [DIMS] is [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\IMSService\DefaultIMSSettings] ■ [GIMS] is [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\IMSService\GlobalIMSSettings] ■ [T] is [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\Temp]
IMS Entry	The entry in the IMS for System and User policies.

Attribute	Description
Values	Possible values that the policy can take on. The default value is indicated with an asterisk "*". The default value is used if the policy is not specified or if the specified value is invalid. The refresh frequency is also indicated here. This indicates when a policy will take effect after it is changed. ■ **Refreshed on use:** Policy read from IMS/registry every time it is used. Changes, for example, take effect immediately. ■ **Refreshed on sync:** Policy read from IMS/registry only on the next synchronization with IMS. ■ **Refreshed on logon:** Policy read from IMS/registry only on the next AccessAgent logon. ■ **Refreshed on startup:** Policy read from IMS/registry only on system startup.
Scope	The scope of applicability of the policy. Values: ■ **System:** Policy is system-wide ■ **Machine:** Policy affects only a specific machine ■ **User:** Policy affects only a specific user System and User policies, as well as selected Machine policies can be configured using AccessAdmin. If pid_machine_policy_override_enabled is 1, machine policies can also be specified as Windows registry entries on individual machines, and they will override the ones defined via AccessAdmin. A policy may be defined for different scopes. For example, pid_desktop_inactivity_mins may define the desktop inactivity time-out duration for a machine or for a user. If this policy is defined for both scopes, we need to define a priority in case the time-out value is different for the machine and for the user. If policy priority is "machine", only the machine policy would be effective.
✱	Frequently used policies

Policies

Description	Registry	IMS Entry	Values	Scope
AccessAgent configuration				
✱ **pid_second_factors_supported_list**				
The 2nd factors supported on this machine. Controls the Wallet registration policy. Also imposes a constraint on the Wallet locks available for logon. *Note: Should the user decide to switch second factors (e.g. from ARFID to RFID), a machine restart is required.*	[DO] "SecondFactorsSupportedList"	Authentication second factors supported	#RFID #ARFID #USB #Fingerprint (currently, only single value allowed, except for simultaneous Fingerprint and RFID support) (refreshed on restart)	Machine
pid_aa_tray_bubble_display_enabled				
Whether to enable Access Agent's bubble pop-ups at the Windows notification area.	[DO] "AATrayBubbleDisplayEnabled"	Enable bubble pop-ups?	*#True #False #0: No *#1: Yes (refreshed on use)	Machine
pid_aa_tray_menu_options_enabled				
Whether to display menu options when user right-clicks AccessAgent icon at the Windows notification area. *Notes:* *1. If policy value is 0, no menu is displayed when AccessAgent icon is right-clicked.* *2. However, if the user double-clicks the AccessAgent icon, normal AccessAgent UI pops up and the user can click on the appropriate option on the AccessAgent UI.*	[DO] "AATrayMenuOptionsEnabled"	Enable right-click menu options?	*#True #False #0: No *#1: Yes (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope

Network

Session Information

pid_session_info_display_freq_secs

Description	Registry	IMS Entry	Values	Scope
Frequency for displaying AccessAgent session information in a bubble pop-up at the Windows notification area. The bubble pops up after every interval, in seconds, specified by this policy. Disable this feature by setting it to 0. *Notes:* *1. Effective only if pid_aa_tray_bubble_display_enabled is 1.* *2. Set policy to 0 to disable the displaying of session information.* *3. If the bubble pop-up will be constantly displayed (unless clicked by user), set this policy to a value less than or equal to pid_session_info_display_dur_secs.* *4. The displayed user name format is determined by pid_logon_user_name_display_option.* *5. If user is logged on with Active Proximity Badge, a warning is shown in the same bubble pop-up if battery is low.*	[DO] "SessionInfoDisplayFreqSecs"	Interval, in minutes, for displaying session information in bubble pop-ups	*0 (refreshed on startup) (0 for no display)	Machine

Logs

pid_log_file_count

Description	Registry	IMS Entry	Values	Scope
Maximum number of AccessAgent log files allowed. Once the maximum number of log files is reached, the oldest log file is deleted to make way for the new log file.	[DO] "LogFileCount"		*10 (refreshed on use)	Machine

pid_log_file_size

Description	Registry	IMS Entry	Values	Scope
Maximum size, in KB, of the log file ("AccessAgent.log"). Once the maximum size is reached, the file is renamed and a new file will be created to store the new logs.	[DO] "LogFileSize"		*1024 (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_log_level				
Level of log details.	[DO] "LogLevel"		*#0: No logging #1: Severe errors only #2: Basic info #3: More info, including SOAP logs #4: Debugging info, including SOAP logs (refreshed on use)	Machine
pid_log_path				
Path to a folder that contains the AccesAgent logs.	[DO] "LogPath"		*<ProgramDir>\logs (refreshed on use)	Machine

Temporary files

pid_temp_path				
Path to a folder that contains the temporary files.	[DO] "TempPath"		*<ProgramDir>\temp (refreshed on use)	Machine

Auto-logon

pid_microsoft_auto_logon_enabled				
Whether to enable auto-logon to Windows on system startup.	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon] "AutoAdminLogon" "ForceAutoLogon" (both entries must be set)		*#0: No #1: Yes (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_microsoft_auto_logon_acct				
Windows account to be used for auto-logon on system startup. *Notes:* *1. Effective only if pid_microsoft_auto_logon_enabled is enabled.* *2. If pid_lusm_session_max>1, a local machine account should be used for auto-logon.*	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon] "DefaultDomainName" "DefaultUserName" "DefaultPassword"		(refreshed on use)	Machine
✱ pid_win_startup_action				
Actions on Windows startup. *Note: This is to enable automatic locking of computer after AutoAdminLogon or ForceAutoLogon.*	[DO] "WinStartupAction"	Windows startup actions	*#0: No action #1: Lock computer (refreshed on use)	Machine

Local user session management policies

pid_lusm_session_replacement_option				
Option for replacing existing user sessions when a new user attempts to log on while the number of concurrent user sessions has already reached the maximum allowed. *Notes:* *1. Effective only if pid_lusm_sessions_max > 1.* *2. Policy value 2 is useful for machines which are used by users in a round-robin fashion.* *3. For policy value 3, the session that has been unlocked the least number of times will be replaced.* *4. For policy value 4, the session that has been least used in terms of total duration will be replaced.* *5. Computation of time for all cases is accurate only to the nearest minute.*	[DO] "LUSMSessionReplacementOption"	Session replacement option	#0: Disallow new user to log on *#1: Replace least recently used (LRU) session #2: Replace most recently used (MRU) session #3: Replace least frequently used (LFU) session #4: Replace least used (LU) session (refreshed on startup)	Machine

Description	Registry	IMS Entry	Values	Scope
✱ pid_lusm_sessions_max				
Maximum number of concurrent user sessions. Set it to 2 or more to enable private desktop. *Notes:* *1. Set policy to 1 to disable Local User Session Management.* *2. To enable Local User Session Management, a value greater than 1 should be specified for this policy in the DeploymentOptions.reg file during AA installation. If this policy is set to a value greater than 1 only after AA is installed, the "Log Off" and "Shut Down" buttons, as well as the Windows hot keys may not be disabled for the very first user who logs on. Also, the buttons and Windows hot keys may remain disabled after AA is uninstalled.* *3. If this policy is set to a value higher than what the system resources can support, the actual number of concurrent user sessions will still be capped by the system resources available.* *4. For optimal performance, it should not be set to a value more than 9.* *5. If Local User Session Management is enabled, pid_logoff_manual_action should be set to 1 (Log off Windows) so that manually logging off AA will be equivalent to logging off the user's desktop session. pid_unlock_with_win_option should be set to 0 as unlock using Windows is not supported for Local User Session Management. Auto admin logon to Windows should also be enabled by setting pid_microsoft_auto_logon_enabled to 1, pid_microsoft_auto_logon_acct to a local machine logon account, and pid_win_startup_action to 1, so as to lock the computer immediately after logon.*	[DO] "LUSMSessions-Max"	Maximum number of concurrent user sessions on a workstation	*1 (refreshed on startup) (from 1 to 12)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_lusm_sia_list				
List of single instance applications (SIA), such as applications that cannot run multiple simultaneous instances in a computer. *Notes:* *1. Effective only if pid_lusm_sessions_max > 1.* *2. When a user starts any application in this list, AccessAgent performs the action specified by pid_lusm_sia_launch_option (if the policy value is not 0) or application's own launch option. Note that these actions are only applicable when the application is launched from a visible desktop and there is another instance of it running in an invisible desktop. If the other instance is running in the same visible desktop, the application will assume its normal behavior.* *3. For each application, the full path should be the full image path of the executable on the disk, ending with ".exe", ".bat", or ".com". It is case-insensitive.* *4. Note that the long path format should be used. For example, for Yahoo Messenger, use "C:\Program Files\Yahoo!\Messenger\YahooMessenger.exe" instead of "C:\progra~1\Yahoo!\messenger\YAHOOM ~1.exe".*	[DO] "LUSMSiaList"	Single instance applications list	Each application occupies 3 lines as follows: Line 1: Full path of executable (for example, C:\Windows\notepad.exe) Line 2: Launch option (see below) Line 3: Display name of the application (for example, Notepad) (empty lines are discarded, and hence, there must be 3 non-empty lines for each application) Launch option is one of the following values: #1: Disallow 2nd instance to start *#2: Log off existing instance #3: Close existing instance #4: Prompt user whether to log off existing instance #5: Prompt user whether to close existing instance (refreshed on startup)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_lusm_sia_launch_option				
Action taken by AccessAgent when user launches a 2nd instance of a single instance application, such as an application that cannot run multiple simultaneous instances in a computer. *Notes:* *1. Effective only if pid_lusm_sessions_max > 1.* *2. If policy value is 0, the each application's own launch option (specified in pid_lusm_sia_list) is used.* *3. Note that these actions are only applicable when the application is launched from a visible desktop and there is another instance of it running in an invisible desktop. If the other instance is running in the same visible desktop, the application will assume its normal behavior.*	[DO] "LUSMSiaLaunchOption"	Action on launching a second instance of a single instance application	#0: Use application's launch option #1: Disallow 2nd instance to start *#2: Log off existing instance #3: Close existing instance #4: Prompt user whether to log off existing instance #5: Prompt user whether to close existing instance (refreshed on startup)	Machine
pid_lusm_generic_accounts_enabled				
Whether to use a pool of generic accounts to create user desktops. *Notes:* *1. Effective only if pid_lusm_sessions_max > 1.* *2. If enabled, generic accounts specified in pid_lusm_generic_accounts_list will be used to create user desktops. This configuration is for deployments where some Encentuate users may not exist in AD, or Encentuate password is not synchronized with AD password.* *3. If enabled, pid_lusm_default_desktop_preserved_enabled must be set to 1.*	[DO] "LUSMGenericAccountsEnabled"	Enable use of generic accounts to create user desktops?	#True *#False *#0: No #1: Yes (refreshed on startup)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_lusm_generic_accounts_list				
List of generic accounts for creating user desktops. *Notes:* *1. Effective only if pid_lusm_sessions_max > 1 and pid_lusm_generic_accounts_enabled is enabled.* *2. Upon machine start-up, AccessAgent writes the obfuscated password into the 4th line of each account, replacing the 3rd line with a fixed mask string "#####encrypted#####".* *3. To add a new account, delete an existing account, or change the user name, domain, or password of an existing account, the entire set of values in this policy must be re-written. AccessAgent will use the new values after the next machine start-up.* *4. If a particular account cannot be validated, this account will be ignored and AccessAgent will write "#####invalid account#####" in the 3rd line of the account.* *5. If the number of valid accounts is less than two, the generic accounts feature will be disabled.* *6. If the number of valid accounts is less than pid_lusm_sessions_max, the actual maximum number of concurrent sessions would be constrained by the number of valid accounts even though resources may allow for more.* *7. Both local machine accounts or domain accounts can be used as generic accounts, but domain accounts are recommended since these accounts do not have to be pre-created on each machine. However, note that the passwords for these accounts should never expire nor be changed, since any password changes will require modifications to this policy.* *8. Users should not unlock directly using generic account credentials as that may lead to an existing user's desktop being unlocked.*	[DO] "LUSMGenericAccountsList"		Each generic account occupies 4 lines as follows: Line 1: User name Line 2: Domain (or machine name for local computer account) Line 3: Password Line 4: == (empty lines are discarded, and hence, there must be 4 non-empty lines for each account) (refreshed on startup)	Machine

Description	Registry	IMS Entry	Values	Scope
Authentication policies				
✱ pid_wallet_authentication_option				
Authentication policy that enforces the combinations of authentication factors that can be used for logon. *Notes:* *1. This policy does not enforce authentication factors to be used for sign-up. Sign-up policy is enforced by pid_second_factors_supported_list and pid_second_factor_for_sign_up_requir ed* *2. RFID includes active proximity badges.*		Wallet authentication policy	#1: Password #2: Password + RFID *#3: USB Key #4: Password + Fingerprint #5: Fingerprint (multiple allowed) (refreshed on logon or unlock by different user, if online) (refreshed on last sync if offline) *Note: #3 is always enabled. #1 enabled => #2 and #4 are also enabled.*	User
✱ pid_mac_auth_enabled				
Whether Mobile ActiveCode authentication is enabled for the user.		Enable Mobile ActiveCode authentication?	#True *#False (refreshed on use)	User
Encentuate password policies				
pid_enc_pwd_is_usb_key_pwd_enabled				
Whether to set Encentuate password to last changed USB Key password. *Notes:* *1. If enabled, Password authenticator's password will always be set to be the same as the USB Key password when the latter is changed.* *2. This policy should be enabled for normal users and disabled for power users.*		Set Encentuate password to last changed USB Key password?	*#True #False (refreshed on next successful password change)	User

Description	Registry	IMS Entry	Values	Scope
Encentuate password aging policies				
pid_enc_pwd_periodic_change_enabled				
Whether to enable password aging, such as periodic password change.		Enable password aging?	#True *#False (refreshed on sync)	System
pid_enc_pwd_change_days				
Maximum password age, in days. It is the period, in days, between two password changes for a Wallet or USB Key. *Note: Effective only if Encentuate password periodic change is enabled.*		Maximum password age, in days	*90 (refreshed on sync)	System
pid_enc_pwd_expiry_reminder_enabled				
Whether to remind user about expiring password. *Note: Effective only if Encentuate password periodic change is enabled.*		Enable password change reminder?	#True *#False (refreshed on sync)	System
pid_enc_pwd_expiry_reminder_days				
Number of days before password expiry to start reminding user. *Note: Effective only if Encentuate password expiry reminder is enabled.*		Number of days before password expiry to start reminding user	*5 (from 1 to 10) (refreshed on sync)	System
pid_enc_pwd_expiry_change_enforced				
Whether to enforce password change on expiry by prompting user to change password before logging on to AccessAgent. *Note: Effective only if Encentuate password periodic change is enabled.*		Enforce password change on expiry?	#True *#False (refreshed on sync)	System
Encentuate password strength policies				
pid_enc_pwd_min_length				
Minimum length of an acceptable Encentuate password. *Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.*		Minimum password length	*6 (from 1 to 99) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_enc_pwd_max_length				
Maximum length of an acceptable Encentuate password. *Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.*		Maximum password length	*20 (from 1 to 99) (refreshed on sync)	System
pid_enc_pwd_min_numerics_length				
Minimum number of numeric characters for an acceptable Encentuate password. *Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.*		Minimum number of numeric characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_enc_pwd_min_alphabets_length				
Minimum number of alphabetic characters for an acceptable Encentuate password. *Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.*		Minimum number of alphabetic characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_enc_pwd_mixed_case_enforced				
Whether to enforce the use of both upper case and lower case characters for the Encentuate password. *Note: Not effective if Encentuate password is AD password is enabled. AD password strength policies will be used instead.*		Enforce the use of both upper case and lower case characters?	#True *#False (refreshed on sync)	System

Self-service password reset policies

✱ pid_selfhelp_password_reset_enabled				
Whether to enable self-service password reset.		Enable self-service password reset?	#True *#False (refreshed on sync)	System
pid_secrets_register_for_selfhelp_max				
The maximum number of secret questions a user should register to enable self-service capability.		Maximum number of secret questions a user should register to enable self-service	*3 (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_secrets_verify_for_selfhelp				
The number of secret questions a user needs to answer for using self-service.		The number of secret questions a user needs to answer to use self-service.	*2 (refreshed on sync)	System
pid_secrets_verify_invalid_trial_count_max				
The maximum number of invalid tries allowed before self-service capability gets locked.		The maximum number of invalid tries allowed before self-service locks out	*6 (refreshed on sync)	System
Self-service authorization code policies				
pid_selfhelp_authcode_enabled				
Whether to enable self-service authorization code issuance using mobile phone.		Enable self-service authorization code issuance?	#True *#False (refreshed on use)	System
pid_selfhelp_authcode_request_from_any_phone_enabled				
Whether to allow self-service authorization code to be requested from any phone. *Note: Effective only if pid_selfhelp_authcode_enabled is True.*		Allow authorization code request from any phone?	#True *#False (refreshed on use)	System
pid_selfhelp_authcode_invalid_trial_count_max				
The maximum number of invalid trials allowed before self-service authorization code request capability gets locked. *Note: Effective only if pid_selfhelp_authcode_enabled is True.*		The maximum number of invalid tries allowed before self-service authorization code request locks out	*6 (refreshed on use)	System
pid_selfhelp_authcode_error_msg_text				
Configurable error message text for self-help authorization code request. *Note: Effective only if pid_selfhelp_authcode_enabled is True.*		Error message text for self-help authorization code request	*An error has occurred. Please contact your Helpdesk. (refreshed on use)	System

Description	Registry	IMS Entry	Values	Scope
pid_selfhelp_authcode_request_help_ text				
Configurable help text for self-service authorization code request. *Notes:* *1. Effective only if pid_selfhelp_authcode_enabled is True.* *2. The help text can be sent to user by the SMS gateway's IMS Bridge, shown by AccessAgent, etc.*		Help text for self-service authorization code request	*You can only request for authorization code using your registered phone. The message format is: UserName UserSecret [RequestCode] (refreshed on use)	System
pid_selfhelp_authcode_issue_msg_text				
Configurable message text for self-help authorization code issuance. *Notes:* *1. Effective only if pid_selfhelp_authcode_enabled is True.* *2. Use $AUTHCODE as place-holder for authorization code.* *3. Use $VALIDITY as place-holder for no. of days for which authorization code is valid.* *4. Use $USAGE as place-holder for string that describes how the authorization code can be used.*		Message text for self-help authorization code issuance	*Your authorization code is $AUTHCODE. You can use it within $VALIDITY days for $USAGE. (refreshed on use)	System
pid_selfhelp_authcode_different_phone_error_msg_text				
Configurable message text to be sent to requesting phone for self-help authorization code if it is different from registered phone and policy is such that only the registered phone can be used. *Notes:* *1. Effective only if pid_selfhelp_authcode_enabled is True and pid_selfhelp_authcode_request_from_any_phone_enabled is False.* *2. Use $PHONE as place-holder for registered phone number.*		Message text sent to requesting phone if it is different from registered phone and only registered phone can be used	*Authorization code can only be requested from your registered phone $PHONE. (refreshed on use)	System

Description	Registry	IMS Entry	Values	Scope
pid_selfhelp_authcode_different_phone_issue_msg_text				
Configurable message text to be sent to requesting phone for self-help authorization code if it is different from registered phone. Notes: *1. Effective only if set to True in pid_selfhelp_authcode_enabled.* *2. Use $PHONE as place-holder for registered phone number.*		Message text sent to requesting phone if it is different from registered phone	*An authorization code has been sent to your registered phone $PHONE. (refreshed on use)	System
pid_selfhelp_authcode_wrong_credentials_error_msg_text				
Configurable message text to be sent to requesting phone for self-help authorization code if any of the requesting credentials is incorrect. Notes: *1. Effective only if set to True in pid_selfhelp_authcode_enabled.* *2. Message text is sent if any of the requesting credentials is incorrect, for example, user name, user secret, request code.*		Message text sent to requesting phone on incorrect credentials	*Incorrect user name, user secret, or request code. Please try again. (refreshed on use)	System

Self-service registration and bypass of 2nd factor policies

✱ pid_selfhelp_second_factor_registration_and_bypass_enabled				
Whether to enable self-service registration and bypass of 2nd factor. Notes: *1. If this policy is enabled, user can bypass the use of 2nd factor for logon by providing registered secrets instead.* *2. Whether authorization code is required for registration of 2nd factors depends on pid_second_factor_registration_option. In cases where authorization code is required, this policy controls whether user can perform the action in a self-service manner by providing registered secrets instead.* *3. If user is not able to provide registered secrets, there is an option to provide an authorization code and primary secret.* 4. Registration of second factors using self-service secrets is not supported for USB Keys.		Enable self-service registration and bypass of 2nd factor?	#True *#False (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope

Wallet policies

pid_wallet_caching_option

Option to control the caching of Wallets. *Note: Offline reset capability (f.k.a. BSK) is automatically enabled if Wallet is cached.*		Wallet caching option	#0: Disallow caching *#1: Ask user #2: Always cache (refreshed on sync)	System

pid_wallet_cache_max

Maximum number of cached Wallets allowed on the machine. *Notes:* *1. If the maximum limit has reached, the least recently used cached Wallet will be deleted before a new Wallet is cached.* *2. Setting a limit on the number of cached Wallets for a shared workstation may improve logon performance.* *3. If biometric authentication is used on a shared workstation, it is recommended that the limit on the number of cached Wallets be set to a value such that the possibility of false acceptance for the biometric device is made negligible. This is because false acceptance may lead to a user logging on to a wrong Wallet.* *4. This policy should be used in conjunction with pid_wallet_cache_max_inactivity_days so that deleted cached Wallets can also be automatically revoked on the IMS Server.* *5. In some deployments, it may be desirable to disable Wallet caching on shared workstations due to security reasons. This policy can be set to 0 to disable caching on a particular machine. In this case, it overrides pid_wallet_caching_option.*	[DO] "WalletCacheMax"	Maximum number of cached Wallets	*999999999 (0 to disable caching) (999999999 for no max limit) (refreshed on use)	Machine

pid_wallet_sync_mins

Interval, in minutes, for periodic synchronization of Wallet with IMS Server. Synchronization is also performed when user logs on to AccessAgent.		Interval, in minutes, for synchronization of Wallet with IMS Server	*30 (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_wallet_cache_max_inactivity_days				
Maximum period of inactivity, in days, allowed for a cached Wallet. After which, the cached Wallet is automatically revoked. *Notes:* *1. If a cached Wallet is not used for a period exceeding the limit imposed by this policy, it is automatically revoked on the IMS Server. AccessAgent will also automatically revoke the cached Wallet when a user attempts to log on to it.* *2. Inactivity is measured from the last synchronization time. Hence, even if a user logs on to a cached Wallet every day, it can still be revoked if it has not been synchronized with the IMS Server for an extended period of time.* *3. If a cached Wallet is revoked, user will only be able to log on if IMS Server is available. There should be no prompt that the Wallet has been revoked, but the option to cache the Wallet may be given (depends on pid_wallet_caching_option).*		Maximum period of inactivity, in days, allowed for a cached Wallet	*999999999 (999999999 for infinity, such as cached Wallets do not expire) (refreshed on sync)	System
pid_wallet_sync_before_logon_enabled				
Whether to enable AccessAgent to perform synchronization with IMS Server before logging on to the Wallet. *Notes:* *1. If this policy is set to 1, AccessAgent performs synchronization before logging on through Windows logon (for EnGINA logon), and before running logon script (for desktop logon and logon from unlock screen).* *2. Due to the longer time needed for USB Key to perform synchronization with IMS Server, this policy is recommended to be set to 0 for USB Key deployments.*	[DO] "WalletSyncBeforeLogonEnabled"	Enable Wallet synchronization before logon?	*#True #False #0: No *#1: Yes (refreshed on use)	Machine
pid_wallet_open_max_tries				
Maximum number of consecutive invalid offline logons before cached Wallet is locked out. Note: This policy does not support Charismathics USB Keys.		Maximum number of consecutive invalid offline logons before cached Wallet is locked out	*5 (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_wallet_editable_items_list				
List of Wallet items that can be edited by the user through AccessAgent.		List of Wallet items that can be edited by the user through AccessAgent.	*#1: Password *#2: Password entry option *#4: Application settings *#8: Delete credential *#16: Add credential (multiple allowed) (refreshed on sync)	User
pid_wallet_inject_pwd_entry_option_default				
Default automatic sign-on password entry option.		Default automatic sign-on password entry option	#1: Automatic logon *#2: Always #3: Ask #4: Never #5: Certificate #6: Use application settings (refreshed on sync)	System
pid_wallet_enterprise_app_never_option_enabled				
Whether the "Never" password entry option is enabled for enterprise authentication services. *Note: User policy, if defined, overrides system policy.*		Enable 'Never' for enterprise authentication services?	*#True #False (refreshed on sync)	User System
pid_wallet_personal_app_sso_enabled				
Whether to enable automatic sign-on for personal authentication services. *Note:* User policy, if defined, overrides system policy.		Enable automatic sign-on for personal authentication services?	*#True #False (refreshed on use for user policy) (refreshed on sync for system policy)	User System
pid_sso_auto_learn_enabled				
Whether auto-learning should be enabled for automatic sign-on to applications.		Enable auto-learning?	*#True #False (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_sso_user_control_enabled				
Whether to allow user to enable/disable automatic sign-on. *Note: If this policy is disabled, the “Enable automatic sign-on” and “Disable automatic sign-on” options will not appear in any part of AccessAgent UI.*	[DO] “SsoUserControlEnabled”	Allow user to enable/disable automatic sign-on?	#0: No *#1: Yes *#True #False (refreshed on sync)	Machine User
pid_accessagent_pwd_display_option				
Option for displaying of application passwords in the Wallet Manager of AccessAgent through the “Show password” option. *Notes:* *1. User is asked to enter Encentuate password before being allowed to display passwords.* *2. Displaying of passwords is not allowed if user is logged on using fingerprint.*		Option for displaying of application passwords in AccessAgent Non-negative integer	*#0: Disallow displaying passwords #1: Allow displaying personal passwords #2: Allow displaying both enterprise and personal passwords (refreshed on sync)	User
pid_accessagent_pwd_export_option				
Option for displaying of application passwords in the Wallet Manager of AccessAgent through the “Show password” option. *Note: User is asked to enter Encentuate password before being allowed to display passwords.*		Option for displaying of application passwords in AccessAgent	#0: Disallow displaying passwords #1: Allow displaying personal passwords *#2: Allow displaying both enterprise and personal passwords (refreshed on sync)	User

Description	Registry	IMS Entry	Values	Scope
pid_migration_stage				
Whether migration from IAM version 1.x to 3.x is in progress and, if so, the current stage of migration. *Notes:* *1. The migration involves the upgrade of IMS Server, AccessAgent, and users' Wallets.* *2. When IMS Server is upgraded, the installer automatically sets the policy value to 1.* *3. This policy should be manually set by Administrator to 2 when all AccessAgent installations have been upgraded.* *4. Users' Wallets are upgraded as and when they log on using upgraded AccessAgent. After all Wallets are upgraded, the policy should be set to 0 so as to optimize IMS Server and AccessAgent performance.* *This can be done automatically by a nightly job that checks whether all Wallets have been upgraded.*		Stage of migration from version 1.x to 3.x	*#0: No migration or migration completed #1: Upgrading IMS Server and AccessAgent #2: IMS Server and AccessAgent fully upgraded (refreshed on sync)	System

Sign-up policies

Description	Registry	IMS Entry	Values	Scope
pid_bind_secret_question_list				
The set of questions that user will choose from during sign-up to provide the secret answer.		Question set for secret	*#What is your mother's maiden name? *#When is your birthday? (multiple allowed) (refreshed on sync)	System
pid_secret_answer_min_length				
Minimum length of an acceptable secret answer.		Minimum length of an acceptable secret answer	*3 (refreshed on sync)	System
pid_secrets_register_for_selfhelp_at_sign_up				
Whether to prompt user to register additional secrets for self-service during sign-up.		Prompt user to register additional secrets for self-service during sign-up?	#True *#False (refreshed on sync) #False	System

Description	Registry	IMS Entry	Values	Scope
pid_secret_option				
Whether the secret is required, should be specified by user during sign-up, or automatically specified using a bind task. *Notes:* *1. This policy applies to users who are signing up or who are logging on for the first time after their accounts have been pre-provisioned.* *2. For policy value 0, user would be assigned a system-defined secret. User would not be prompted for secret when performing actions that require it, for example, reset password, and offline recovery. Customer should understand the security vulnerabilities before deciding to implement such a configuration.* *3. Currently, if policy value is changed from 1 to 0, users will be automatically migrated to system-defined secret when they log on to AccessAgent. However, there is no support for migration from policy value 0 to 1.*		Option for specifying secret	#0: Secret not required *#1: Secret required, and user must specify during sign-up (refreshed on sync)	System
pid_second_factor_for_sign_up_required				
Whether 2nd factor is required during sign-up. *Notes:* *1. Effective only if second factors supported list is not empty, in which case, any one of the supported 2nd factors can be used for sign-up. There will be one UI dialog asking for user to present any one of the supported 2nd factors.* *2. If policy value is 1, sign-up fails if 2nd factor is not presented.*	[DO] "SecondFactorForSignUpRequired"	Require authentication second factor during sign-up?	#True *#False *#0: Not required #1: Required (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
✱ pid_automatic_sign_up_enabled				
Whether to enable automatic sign up. *Notes:* *1. This policy should be set to 1 if* Encentuate password is synchronized with Active Directory password. *2. pid_engina_welcome_text and pid_unlock_text should be modified accordingly if this policy is set to 1.* *3. If this policy is set to 1, the "Sign up" option will not be available on both the AccessAgent UI and AccessAgent Tray menu; user will not be prompted to sign up if attempting to log on to an unregistered user name; user will not be prompted to confirm having signed up if an unregistered 2nd factor is presented.*	[DO] "AutomaticSignUpEnabled"	Enable automatic sign-up?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine

Policy templates

pid_policy_template_default

The default user policy template to be applied.		Default policy template	*default user policy template (refreshed on use)	System

pid_machine_policy_template_default

The default machine policy template to be applied.		Default machine policy template	*default machine policy template (refreshed on use)	System

ActiveCode policies

pid_mac_max_validity_count

Maximum number of Mobile ActiveCodes that may be valid for a user at any time.		Maximum number of Mobile Active Codes that may be valid for a user at any time.	*3 (from 1 to 7) (refreshed on use)	System

Description	Registry	IMS Entry	Values	Scope
pid_activecode_bypass_option				
Option for ActiveCode authentication bypass. *Note: Can be used for bypassing both Mobile ActiveCode and OTP ActiveCode (AccessAgent-OTP and on-board OTP).*		ActiveCode bypass option	#1: Authorization code and Encentuate password #2: Authorization code and enterprise account password #4: Authorization code and secret (multiple allowed) (0 for "No bypass") (refreshed on use)	System
pid_activecode_append_secret_option				
Option for appending a secret to Mobile ActiveCode. *Note: The order is also specified in the policy values.*		Option for appending a secret to Mobile ActiveCode	*#0: MAC only (no appending of secret) #1: MAC + Encentuate password #2: MAC + Enterprise account password #3: MAC + Administrator-assigned secret #4: Encentuate password + MAC #5: Enterprise account password + MAC #6: Administrator-assigned secret + MAC (refreshed on use)	System

Description	Registry	IMS Entry	Values	Scope
pid_otp_append_secret_option				
Option for appending a secret to OTP (time-based) and OTP (OATH). *Notes:* *1. Not applicable to AA-OTP and USB Key on-board OTP.* *2. The order is also specified in the policy values.*		Option for appending a secret to OTP (time-based) and OTP (OATH)	*#0: OTP only (no appending of secret) #1: OTP + Encentuate password #2: OTP + Enterprise account password #3: OTP + Administrator-assigned secret #4: Encentuate password + OTP #5: Enterprise account password + OTP #6: Administrator-assigned secret + OTP (refreshed on use)	System
pid_otp_reset_sample_count				
Number of consecutive OTPs to be obtained from user for resetting an OTP (OATH) token.		Number of consecutive OTPs needed for resetting an OTP (OATH) token	*3 (from 1 to 5) (refreshed on sync)	System
pid_activecode_admin_assigned_secret_name				
Identity attribute name of the Administrator-assigned secret, for appending to ActiveCode. *Notes:* *1. Can be used for both Mobile ActiveCode and OTP ActiveCode (AccessAgent-OTP and on-board OTP).* *2. Effective only if ActiveCode append secret option is 3.*		Identity attribute name of the Administrator-assigned secret	(refreshed on use)	System

AccessAssistant and Web Workplace policies

Description	Registry	IMS Entry	Values	Scope
pid_accessanywhere_enabled				
Whether user is allowed to use AccessAssistant.		Allow access to Wallet from AccessAssistant?	*#True #False (refreshed on use)	User

Description	Registry	IMS Entry	Values	Scope
✱ **pid_accessanywhere_second_factor_enabled**				
Whether user is required to authenticate using second factor when using AccessAssistant.		Second factor authentication required for AccessAssistant?	*#True #False (refreshed on use)	User
pid_accessanywhere_personal_app_enabled				
Whether to display personal authentication services in AccessAssistant and Web Workplace. *Note: Effective only if pid_accessanywhere_enabled is True.*		Display personal authentication services in AccessAssistant and Web Workplace?	#True *#False (refreshed on sync)	User
pid_accessanywhere_edit_user_profile_enabled				
Whether the user profile can be edited by user in AccessAssistant and Web Workplace.		Enable editing of user profile in AccessAssistant and Web Workplace?	#True *#False (refreshed on sync)	System
pid_accessanywhere_second_factor_default				
The user's default second authentication factor for logging on to AccessAssistant and Web Workplace. *Notes:* *1. Effective only if pid_accessanywhere_enabled and pid_accessanywhere_second_factor_enabled are True.* *2. After user name and password are entered, AccessAssistant or Web Workplace will prompt for the default 2nd factor. User can still click on links to use other 2nd factors.* *3. If the default 2nd factor is MAC, a MAC will automatically be sent to the user via the preferred channel right after entering user name and password. There will be a message indicating where the MAC has been sent to, and links for the user to request for MAC to be sent to another channel.* User should be able to change preferred MAC channel through the user profile settings page.		Default second authentication factor for AccessAssistant and Web Workplace	*#1: Authorization code #2: MAC #3: OTP (time-based) (refreshed on use)	User

Description	Registry	IMS Entry	Values	Scope
pid_accessanywhere_app_sso_enabled				
Whether the user can perform automatic sign-on to applications through AccessAssistant.		Enable automatic sign-on to applications in AccessAssistant?	#True *#False (refreshed on sync)	System
pid_accessanywhere_password_display_option				
Option for display of application passwords in AccessAssistant.		Password display option in AccessAssistant	#0: Disable viewing of passwords #1: Display password, no option to copy to clipboard *#2: Display password by default, with option to copy to clipboard #3: Copy to clipboard by default, with option to display password (refreshed on sync)	System

AccessAudit policies

pid_audit_custom_events_list				
List of custom audit event codes and their corresponding display names. *Note: AccessProfiles should be written to detect the events and submit appropriate custom audit logs.*		List of custom audit events	Each custom event is represented by one string of the form: event_code,display_name event_code should be a hexadecimal value in the range: 0x43015000 to 0x43015FFF (multiple allowed) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope

AccessAgent policies

EnGINA policies

pid_engina_winlogon_option_enabled

Description	Registry	IMS Entry	Values	Scope
Whether to enable the option to go to Windows logon directly from EnGINA.	[DO] "EnginaWinlogonOptionEnabled"	Allow logon bypass through Windows?	*#True #False *#1: Yes #0: No (refreshed on use)	Machine

pid_engina_app_launch_enabled

Description	Registry	IMS Entry	Values	Scope
Whether to enable the launching of an application from EnGINA welcome or locked screen.	[DO] "EnginaAppLaunchEnabled"	Enable application launch from EnGINA?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine

pid_engina_app_launch_label

Description	Registry	IMS Entry	Values	Scope
Display label for the link on EnGINA welcome or locked screen, for launching an application. *Note: Effective only if pid_engina_app_launch_enabled is 1.*	[DO] "EnginaAppLaunchLabel"	Display label for application launch	(refreshed on use)	Machine

pid_engina_app_launch_cmd

Description	Registry	IMS Entry	Values	Scope
Command line for launching an application from EnGINA welcome or locked screen. *Notes:* *1. Effective only if pid_engina_app_launch_enabled is 1.* *2. If the application is launched from welcome screen, the owner of the process for the application will be "System".* *3. If the application is launched from locked screen, the owner of the process for the application will be "currently logged on desktop user".*	[DO] "EnginaAppLaunchCmd"	Command line for application launch	(refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_engina_bypass_hot_key_enabled				
Whether EnGINA Bypass Hot Key is enabled. *Notes:* *1. If enabled, user can press the EnGINA Bypass Hot Key sequence to bypass EnGINA and go to Windows to log on or unlock.* *2. Hot Key is accepted at any of the following EnGINA states: Welcome, Log On, Computer Locked, Unlock This Computer.* *3. If Hot Key is pressed at computer locked screen, AccessAgent will not ask the user for confirmation on whether to log off previous user, even though there can be a previous user logged on to the computer. Microsoft GINA will be presented to user, but it will allow unlocking only by the same user or Administrator.*	[DO] "EnginaBypass-HotKeyEnabled"	Enable EnGINA Bypass Hot Key?	*#1: Yes #0: No *#True #False (refreshed on startup)	Machine System
pid_engina_bypass_hot_key_sequence				
The EnGINA Bypass Hot Key sequence. *Note:* *Effective only if pid_engina_bypass_hot_key_enabled is enabled.*	[DO] "EnginaBypass-HotKeySequence"	EnGINA Bypass Hot Key sequence	*#Ctrl *#Alt *#Home (max 3 keys from set of: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E}, except for Ctrl-Alt-Del, which is not allowed) (2 of the keys in this set should be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt) (refreshed on startup)	Machine System

Description	Registry	IMS Entry	Values	Scope
pid_engina_bypass_automatic_enabled				
Whether automatic EnGINA Bypass is enabled. *Notes:* *1. If enabled, IMS Server is not contactable, and user's Wallet is not cached, AccessAgent will automatically bypass EnGINA and show Microsoft GINA when user attempts to log on or unlock. A configurable text message is shown (pid_engina_bypass_automatic_text) in a prompt with an OK button.* *2. If pid_unlock_option is 4, AccessAgent will first prompt whether to log off previous user. If user clicks Yes, pid_enc_pwd_is_ad_pwd_enabled is True, IMS Server is not contactable, and user's Wallet is not cached, AccessAgent will prompt user with configurable text message (pid_engina_bypass_automatic_text). After user clicks OK, AccessAgent will log off the previous user's desktop and automatically bring the new user to the Microsoft GINA's logon screen.* *3. This feature does not support logon with 2nd factors.*	[DO] "EnginaBypassAutomaticEnabled"	Enable automatic EnGINA bypass?	#True *#False #1: Yes *#0: No (refreshed on startup)	Machine
pid_engina_bypass_automatic_text				
Configurable text message for automatic EnGINA bypass		Message for automatic EnGINA bypass	*AccessAgent is currently unable to connect to the IMS Server to log on to your Wallet. You may proceed to log on to Windows but automatic sign-on will be disabled. (refreshed on sync)	System

Desktop inactivity policies

Description	Registry	IMS Entry	Values	Scope
✱ pid_desktop_inactivity_mins				
Desktop inactivity duration, in minutes, after which AccessAgent may perform a set of actions.	[DO] "DesktopInactivityMins"	Desktop inactivity duration, in minutes	*30 (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System

Description	Registry	IMS Entry	Values	Scope
✱ pid_desktop_inactivity_action				
Actions to be performed by AccessAgent after a period of desktop inactivity. *Notes:* *1. This policy is ineffective if computer is already locked. In that case, locked inactivity action would be effective.* *2. If user is not logged on to Wallet, the "log off Wallet" actions for policy values 2 and 5 will not be performed.*	[DO] "DesktopInactivityAction"	Desktop inactivity actions	*#0: No action #1: Log off Windows #2: Log off Wallet #4: Lock computer #5: Log off Wallet and lock computer (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System
pid_desktop_inactivity_action_countdown_secs				
Confirmation countdown duration, in seconds, for desktop inactivity.	[DO] "DesktopInactivityActionCountdownSecs"	Confirmation countdown duration, in seconds, for desktop inactivity	*5 (0 to disable confirmation countdown) (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System
pid_win_screensaver_action				
Actions to be performed by AccessAgent on Windows screen saver activation. *Notes:* *1. If this policy triggers a computer lock, desktop inactivity action becomes ineffective.* *2. If this policy triggers a screen saver without password protection, desktop inactivity action would still remain effective while screen saver is on.* *3. This policy allows a 2-level desktop inactivity behavior. If this policy is set to 1, desktop inactivity mins is set to 4, and the Windows screen saver is set to time-out in 2 minutes and not password protected, then the computer will show screen saver after 2 minutes of idling and be locked after an additional 2 minutes of idling.*	[DO] "WinScreensaverAction"	Actions on Windows screen saver activation	#0: Disable Windows screen saver #1: If screen saver is password protected, lock computer, else show normal screen saver *#2: Lock computer (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System
pid_locked_computer_inactivity_mins				
Locked computer inactivity duration, in minutes, after which AccessAgent may perform a set of actions.	[DO] "LockedComputerInactivityMins"	Locked computer inactivity duration, in minutes	*30 (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System

Description	Registry	IMS Entry	Values	Scope
pid_locked_computer_inactivity_action				
Actions to be performed by AccessAgent after a period of desktop inactivity while computer is locked and user is logged on to Wallet. *Notes:* 1. Effective only if pid_lusm_sessions_max = 1. 2. This policy is effective only if EnGINA screen lock is shown.	[DO] “LockedComputerInactivityAction”	Locked computer inactivity actions when user is logged on to Wallet	*#0: No action #1: Log off Windows (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System
Lock policies				
pid_lock_option				
Type of screen lock to be used when computer is locked. *Notes:* 1. If pid_lusm_sessions_max > 1, only policy 1 (EnGINA screen lock) is supported. *2. From transparent screen lock, user can trigger an unlock or switch user by presenting a 2nd factor.* *3. From transparent screen lock, AccessAgent UI is displayed when Encentuate Hot Key is pressed. From this screen, user can manually log off AccessAgent, which will unlock the computer, and actions specified by pid_logoff_manual_action will be performed.* *The “log off” action will be available regardless of the setting for pid_logoff_manual_while_locked_option_enabled.* *4. Even after transparent screen lock is activated, the action specified by pid_desktop_inactivity_action will still be carried out after a period of desktop inactivity has elapsed. Hence, pid_desktop_inactivity_action is recommended to be set to 4.*	[DO] “LockOption	Screen lock option	#1: EnGINA screen lock #2: Transparent screen lock (refreshed on use) PublicAdmin	Machine
pid_lock_transparent_text				
Configurable text for transparent screen lock. *Note: Effective only if pid_lock_option is 2.*	[DO] “LockTransparentText”	Transparent screen lock message	*Tap your RFID card or Ctrl-Alt-E to unlock. (text box takes about 40 chars) (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_lock_transparent_hot_key_enabled				
Whether the "Ctrl-Esc" Hot Key sequence is enabled during transparent screen lock. *Notes:* *1. Effective only if pid_lock_option is 2 and transparent screen lock is shown.* *2. If enabled, this Hot Key is equivalent to the Encentuate Hot Key when computer is locked. When pressed, AccessAgent UI is shown on the transparent screen lock.* *3. This additional Hot Key is useful for remote access systems (for example, LANDesk) that can send only limited key sequences.*	[DO] "LockTransparentHotKeyEnabled"	Enable transparent screen lock hot key?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
Lock/Unlock policies				
✱ pid_unlock_option				
Unlock computer policy for controlling who is allowed to unlock a computer when it has been locked by a user who is logged on to AccessAgent. *Notes:* 1. Effective only if pid_lusm_sessions_max = 1. 2. Same user refers to the same Encentuate user who locked the computer (i.e., same user name). 3. Admin refers to Windows user with Administrator privilege on that computer, i.e., the Wallet should contain Windows credentials of an Admin user on that computer. 4. This policy is ignored if pid_lock_option = 2 (transparent screen lock). In transparent screen lock mode, any user is always allowed to unlock the computer. 5. For policy 3, if a different user tries to unlock, AA unlocks computer and brings the user to the current desktop, but it logs on to new Wallet after logging off the old one. 6. For policy 4, only the same user can unlock computer and bring the user to the current desktop. For any other users, AA logs off from old desktop and logs on to new Wallet. AA shall not require user to present 2nd factor one more time. If new Wallet does not have a desktop account on the computer, user would need to log on to Windows too. This option is currently not supported for ARFID.	[DO] "UnlockOption"	Unlock computer policy	#1: Only the same user can unlock *#3: Any user with or without current desktop account in Wallet can unlock #4: Only the same user can unlock, but different user can relog on to Windows (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_unlock_with_win_option				
Option for unlocking using Windows unlock. *Notes:* *1. Policy should be set to 1 for personal workstations, if desired, and 2 for shared workstations.* 2. Policy should be set to 0 if pid_lusm_sessions_max > 1. *3. AccessAgent is logged off when computer is unlocked using Windows unlock.*	[DO] "UnlockWithWinOption"	Option for allowing unlock bypass through Windows	#0: Disabled *#1: Windows unlock is always available #2: Windows unlock is available only if AccessAgent is not logged on (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_unlock_different_user_action_countdown_secs				
Confirmation countdown duration, in seconds, for unlocking by a different user. *Notes:* 1. Effective only if pid_lusm_sessions_max = 1. *2. Effective when a user attempts to unlock computer while another user has already been logged on to AccessAgent.* *3. If policy value is non-zero, user can click on the prompt to cancel switch user. If user does not confirm, AccessAgent will proceed to unlock the computer.*	[DO] "UnlockDifferentUserAction-CountdownSecs"	Confirmation countdown duration, in seconds, for unlocking by a different user	*0 (0 to disable confirmation countdown) (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_script_unlock_enabled				
Whether to enable running of unlock script when user unlocks an existing AccessAgent session. *Notes:* *1. The unlock script is only executed if user already has an existing AccessAgent session and is unlocking it.* *2. The unlock script is not executed if user is unlocking a shared workstation that is logged on with a generic Windows account, and not currently logged on to AccessAgent. In this case, the logon script (see pid_script_logon_enabled) will be executed instead.* *3. The unlock script can be used in Local User Session Management (LUSM) to auto-launch single-instance applications that may have been terminated by other users who are logged on to the same workstation.* *4. Unlock script is not supported if pid_lock_option is 2 (such as transparent screen lock is used).*		Enable unlock script when user unlocks an existing AccessAgent session?	#True *#False (refreshed on sync)	User
pid_script_unlock_type				
Type of unlock script to be run. *Notes:* *1. Effective only if pid_script_unlock_enabled is enabled.* *2. See pid_script_unlock_enabled.*		Unlock script type	*#1: Batch #2: VBScript (refreshed on sync)	User

Description	Registry	IMS Entry	Values	Scope
pid_script_unlock_code				
Source code of unlock script to be run. *Notes:* *1. Effective only if pid_script_unlock_enabled is enabled.* *2. See pid_script_unlock_enabled.*		Unlock script code	(refreshed on sync)	User
pid_script_lock_enabled				
Whether to enable running of lock script during locking of the user's AccessAgent session. *Notes:* *1. The lock script is only executed if user's session is currently visible during locking. That is, in Local User Session Management (LUSM), currently invisible user sessions will not have lock script executed.* *2. The lock script is executed regardless of whether the locking is due to desktop inactivity or manually triggered (for example, pressing Win-L or tapping RFID card).* *3. The lock script is useful for closing applications when a "guest" AccessAgent session is being locked. It can also be used in conjunction with the unlock script in a Local User Session Management (LUSM) scenario to record any single-instance applications that may be running before locking, which may have to be relaunched during unlock.*		Enable lock script during locking of the user's AccessAgent session?	#True *#False (refreshed on sync)	User
pid_script_lock_type				
Type of lock script to be run. *Notes:* *1. Effective only if pid_script_lock_enabled is enabled.* *2. See pid_script_lock_enabled.*		Lock script type	*#1: Batch #2: VBScript (refreshed on sync)	User
pid_script_lock_code				
Source code of lock script to be run. *Notes:* *1. Effective only if pid_script_lock_enabled is enabled.* *2. See pid_script_lock_enabled.*		Lock script code	(refreshed on sync)	User

Description	Registry	IMS Entry	Values	Scope
USB Key policies				
pid_usb_key_removal_action				
Actions to be performed when USB Key is removed. *Note:* *Currently, this is supported only if pid_lusm_sessions_max = 1. In future, if pid_lusm_sessions_max > 1, AA with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.*	[DO] "UsbKeyRemovalAction"	USB Key removal actions	#1: Log off Windows #2: Log off Wallet *#4: Lock computer #5: Log off Wallet and lock computer (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
RFID policies				
✱ pid_rfid_tap_same_action				
Actions to be performed by AccessAgent when the currently logged on user taps the RFID card on desktop. *Notes:* *1. This policy is not applicable if the user did not log on using RFID.* *2. If pid_lusm_sessions_max > 1, AA with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.*	[DO] "RfidTapSameAction"	Actions on tapping same RFID on desktop	*#0: No action #1: Log off Windows #2: Log off Wallet #4: Lock computer #5: Log off Wallet and lock computer (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_rfid_tap_same_action_countdown_secs				
Confirmation countdown duration, in seconds, for tapping same RFID on desktop.	[DO] "RfidTapSameActionCountdownSecs"	Confirmation countdown duration, in seconds, for tapping same RFID on desktop	*5 (0 to disable confirmation countdown: not recommended to prevent accidental double detection of RFID tap) (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User

Description	Registry	IMS Entry	Values	Scope
✱ pid_rfid_only_unlock_enabled				
Whether to allow RFID-only unlock (without password) by the same user who locked the computer, if unlock happens within the duration specified by pid_rfid_only_unlock_timeout_secs. Note: *Also applies to Active Proximity Badge. But if pid_lusm_sessions_max > 1, the Active Proximity Badge only unlock is applicable only for the last visible user desktop.*	[DO] "RfidOnlyUnlockEnabled"	Enable RFID-only unlock?	#1: Yes *#0: No #True *#False (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
✱ pid_rfid_only_unlock_timeout_secs				
Time expiry, in seconds, for RFID-only unlock. After this duration (timed from last lock), RFID only unlock will not be allowed. Notes: *1. Effective only if pid_rfid_only_unlock_enabled is enabled.* *2. Also applies to Active Proximity Badge.*	[DO] "RfidOnlyUnlock-TimeoutSecs"	Time expiry, in seconds, for RFID-only unlock	*0 (0 to disable expiry, such as always allow RFID-only unlock) (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
✱ pid_rfid_only_logon_enabled				
Whether to allow RFID-only logon (without password) by a user who has recently logged on using RFID and password on the same or another computer, if logon happens within the duration specified by pid_rfid_only_logon_timeout_mins. Notes: *1. RFID-only logon will only work if IMS Server is online and user has an existing cached Wallet on the computer.* *2. RFID-only logon is tied to the specific RFID card used for logon. If user has two RFID cards and card #1 was used to log on, user can use RFID-only logon only with card #1. If attempting to log on with card #2, user should be prompted for password.* *3. For better security, pid_wallet_cache_max_inactivity_days should be used to clear inactive Wallets, so that exposure of RFID-only logon is only limited to those computers that a particular user frequently uses.* *4. RFID-only logon is not supported if pid_lusm_sessions_max > 1.*	[DO] "RfidOnlyLogonEnabled"	Enable RFID-only logon?	#True *#False #1: Yes *#0: No (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
✱ pid_rfid_only_logon_timeout_mins				
Time expiry, in minutes, for RFID-only logon. After this duration (timed from last logon with RFID and password), RFID-only logon will not be allowed. *Notes:* *1. Effective only if pid_rfid_only_logon_enabled is enabled.* *2. Time-out is refreshed upon every logon to AccessAgent with RFID and password.*		Time expiry, in minutes, for RFID-only logon	*480 (0 to disable RFID-only logon) (refreshed on sync)	User
✱ pid_rfid_tap_different_action				
Actions to be performed by AccessAgent when an RFID card that does not belong to the currently logged on user is tapped on desktop. *Notes:* *1. If pid_rfid_display_utility_enabled is 1, this policy is not effective.* *2. This policy is applicable even if the current user did not use RFID to log on.* *3. For policy value 8, AccessAgent shall not require new user to tap RFID again after logging off from Windows.* *4. If pid_lusm_sessions_max > 1, AccessAgent with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen. AccessAgent with policy value 6 (Switch user) will attempt to create a user desktop session for the new user. AccessAgent with policy value 8 (Log off Windows and log on as new user) will log off the current user's desktop session and create a user desktop session for the new user.*	[DO] “RfidTapDifferentAction”	Actions on tapping different RFID on desktop	*#0: No action #4: Lock computer #5: Log off Wallet and lock computer #6: Switch user #8: Log off Windows and log on as new user (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User

Description	Registry	IMS Entry	Values	Scope
pid_rfid_tap_different_action_countdown_secs				
Confirmation countdown duration, in seconds, for tapping different RFID on desktop.	[DO] "RfidTapDifferentActionCountdownSecs"	Confirmation countdown duration, in seconds, for tapping different RFID on desktop	*5 (0 to disable confirmation countdown: recommended only when RFID tap different action is 6, to prevent accidental double detection of RFID tap) (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_rfid_display_utility_enabled				
Whether to display the registration status of an RFID card that does not belong to the currently logged on user when it is tapped on desktop. *Notes:* *1. If policy value is 1, this policy overrides pid_rfid_tap_different_action. If RFID card is registered, the user name is displayed in a prompt.* *2. This display utility will only work when AccessAgent is logged on.*	[DO] "RfidDisplayUtilityEnabled"	Enable RFID display utility?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine
Active Proximity Badge policies				
pid_arfid_presentation_range_max				
Maximum range for recognizing that an active proximity badge is presented.	[DO] "ArfidPresentationRangeMax"	Maximum range for recognizing that an active proximity badge is presented	*3 (from 1 to 16) (should be Active Proximity Badge removal range minimum - 3) (3 for near, 5 for medium, 7 for far) (refreshed on use)	Machine System
pid_arfid_removal_range_min				
Minimum range for recognizing that an active proximity badge is removed.	[DO] "ArfidRemovalRangeMin"	Minimum range for recognizing that an active proximity badge is removed	*7 (from 4 to 19) (should be Active Proximity Badge presentation range max + 3) (7 for near, 9 for medium, 13 for far) (refreshed on use)	Machine System

Description	Registry	IMS Entry	Values	Scope
Fingerprint policies				
✱ pid_fingerprint_tap_same_action				
Actions to be performed by AccessAgent when the currently logged on user taps finger on the reader. *Note:* *1. This policy is not applicable if the user did not log on using fingerprint.* *2. Currently, this is supported only if pid_lusm_sessions_max = 1. In future, if pid_lusm_sessions_max > 1, AA with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.]*	[DO] "FingerprintTapSameAction"	Actions on tapping same finger on desktop	*#0: No action #1: Log off Windows #2: Log off Wallet #4: Lock computer #5: Log off Wallet and lock computer (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_fingerprint_tap_same_action_countdown_secs				
Confirmation countdown duration, in seconds, for tapping same finger on desktop.	[DO] "FingerprintTapSameAction-CountdownSecs"	Confirmation countdown duration, in seconds, for tapping same finger on desktop	*5 (0 to disable confirmation countdown: not recommended to prevent accidental double detection of finger tap) (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_fingerprint_tap_different_action_countdown_secs				
Confirmation countdown duration, in seconds, for tapping different finger on desktop.	[DO] "FingerprintTapDifferentAction-CountdownSecs"	Confirmation countdown duration, in seconds, for tapping different finger on desktop	*5 (0 to disable confirmation countdown: recommended only when fingerprint tap different action is 6, to prevent accidental double detection of finger tap) (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User

Description	Registry	IMS Entry	Values	Scope
✱ pid_fingerprint_tap_different_action				
Actions to be performed by AccessAgent when a finger that does not belong to the currently logged on user is tapped on desktop. *Notes:* *1. This policy is applicable even if the current user did not use fingerprint to log on.* 2. For policy value 8, AA shall not require new user to tap RFID again after logging off from Windows. 3. Currently, this is supported only if pid_lusm_sessions_max = 1. In future, if pid_lusm_sessions_max > 1, AccessAgent with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen. AccessAgent with policy value 6 (Switch user) will attempt to create a user desktop session for the new user. AccessAgent with policy value 8 (Log off Windows and log on as new user) will log off the current user's desktop session and create a user desktop session for the new user.	[DO] "FingerprintTapDifferentAction"	Actions on tapping different finger on desktop	*#0: No action #4: Lock computer #5: Log off Wallet and lock computer #6: Switch user #8: Log off Windows and log on as new user (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_fingerprint_registration_max				
Maximum number of fingerprints that each user should be allowed to register. *Note: If the value of this policy is reduced, a user who has already registered more fingerprints than allowed by the new policy value will still be allowed to log on with any of the fingerprints that have been registered. However, if attempting to register a new fingerprint, an existing fingerprint will have to be replaced. The user will not be able to increase the number of fingerprints registered.*		Maximum number of fingerprints that can be registered per user	(from 1 to 10) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
Terminal Server/**Roaming session policies**				
pid_machine_type_ts				
Whether the machine is a Terminal Server or Citrix server. *Notes:* *This policy should be set to 1 on the remote AccessAgent (such as on the Terminal Server or Citrix server).* *If this policy is 1, AccessAgent behaves as a remote AccessAgent:* *1. It synchronizes itself with the local AccessAgent.* *2. Second factors supported list is not effective. It is treated as an empty list.* *3. "Lock computer" options from the WNA and AccessAgent UI are disabled, if logon to remote AccessAgent is performed using credentials submitted by local AccessAgent.* *4. Uses Terminal Service second factor bypass option to determine its behavior when user's authentication policy requires 2nd factor for logon.* The following combinations of policy settings are not supported (behavior is unpredictable): - policy value 0 on a Terminal Server or Citrix server installation - policy value 1 on a client machine installation.	[DO] "MachineTypeTS"		#1: Machine is Terminal Server *#0: Machine is not Terminal Server (refreshed on startup)	Machine
pid_ts_logon_prompt_enabled				
Whether to launch AccessAgent logon dialog if AccessAgent is not logged on while a Terminal Server session or Citrix application is launched. *Note: This policy should be set on the remote AccessAgent (such as on the Terminal Server or Citrix server).*	[DO] "TSLogon-PromptEnabled"	Enable auto-launching of AccessAgent logon prompt?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine
pid_ts_logon_cache_enabled				
Whether to cache the Wallet logon credentials in AD roaming profile so that AccessAgent can automatically log on to Wallet. *Note: This policy should be set on the remote AccessAgent (such as on the Terminal Server or Citrix server).*	[DO] "TSLogon-CacheEnabled"	Enable caching of Wallet logon credentials?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_ts_lock_local_computer_action				
Option to disconnect the Terminal Server or Citrix session, and/or log off the remote AccessAgent while locking the local computer.		Actions on remote session while locking local computer	#0: No action #1: Disconnect remote session #2: Log off remote AccessAgent and disconnect remote session #3: Log off remote session #4: Log off remote AccessAgent (refreshed on sync)	User
pid_ts_logoff_local_session_action				
Option to disconnect the Terminal Server or Citrix session, and/or log off the remote AccessAgent before logging off the local AccessAgent.		Actions on remote session before logging off local session	*#0: No action #1: Disconnect remote session #2: Log off remote AccessAgent and disconnect remote session #3: Log off remote session #4: Log off remote AccessAgent (refreshed on sync)	User
pid_ts_engina_logon_no_local_session_enabled				
Whether to use EnGINA logon or Microsoft GINA logon for the Terminal Server session, when there is no local AccessAgent session. *Notes:* *1. This policy should be set on the remote AccessAgent (such as on the Terminal Server or Citrix server).* *2. This policy should be set to 0 on Citrix servers.*	[DO] "TSEnginaLogon-NoLocalSession-Enabled"	Use EnGINA logon when there is no local AccessAgent session?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_ts_logoff_on_reconnect_no_local_session_enabled				
Whether to log off remote AccessAgent when user, with no local AccessAgent session, reconnects to an existing session on Terminal Server or Citrix server. *Notes:* *1. This policy should be set on the remote AccessAgent (such as on the Terminal Server or Citrix server).* *2. This policy is effective only if there is no local AccessAgent session on the user's client machine.* *3. This policy should be set to 1 if users use a generic Windows account to log on to remote session. Logging off the remote AccessAgent ensures that the next user is not able to use the previous user's Wallet and applications.* *4. The usual logoff actions (auto-logoff of applications and running of logoff script) are performed when remote AccessAgent is logged off.* *5. If pid_ts_logon_prompt_enabled is set to 1, remote AccessAgent prompts user to log on after the previous user has been logged off.*	[DO] "TSLogoffOnReconnectNoLocalSessionEnabled"	Log off remote AccessAgent when reconnecting from workstation without local AccessAgent session?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_ts_delay_app_launch_enabled				
Whether to enable the delaying of application launch for Citrix server. *Notes:* *1. Currently, this feature is only applicable to Citrix. It is not applicable to Terminal Server access using RDP.* *2. This policy should be set on the remote AccessAgent (such as on the Citrix server).* *3. If this feature is not enabled for an application, user may see the application's logon prompt first before remote AccessAgent is ready to perform automatic sign-on, and hence, causing some confusion to the user. Enabling this feature for an application will ensure that remote AccessAgent is ready to perform automatic sign-on when user sees the logon prompt.* *4. This feature is only applicable to the use case of having local AccessAgent automatically log on to remote AccessAgent. If there is no local AccessAgent or local AccessAgent is not logged on, application launch will not be delayed even if this feature is enabled.*	[DO] "TSDelayAppLaunchEnabled"	Delay application launch for Citrix server?	#True *#False #1: Yes *#0: No (refreshed on use)	Machine
pid_ts_delay_app_launch_exe_list				
The list of applications which should be delayed from launching until remote AccessAgent is ready to perform automatic sign-on. *Notes:* *1. This policy should be set on the remote AccessAgent (such as on the Citrix server).* *2. Effective only if pid_ts_delay_app_launch_enabled is enabled.* *3. Each application should be indicated by its executable name (for example, "notepad.exe").*	[DO] "TSDelayAppLaunchExeList"	Applications to be delayed from launching on Citrix server	(refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_ts_start_aa_no_local_aa_enabled				
Whether to start remote AccessAgent while a published application is launched through Terminal Server or Citrix, and if local AccessAgent is not present. *Notes:* *1. This policy should be set on the remote AccessAgent (such as on the Terminal Server or Citrix server).* 2. This policy only applies to launching of published applications. If a remote desktop is launched, remote AA will always be started. 3. *For policy value 0, users will not be able to log on to remote AccessAgent from machines that do not have local AccessAgent installed (for example, home or Internet café).*	[DO] "TSStartAANoLocalAAEnabled"	Launch remote AccessAgent even if local AccessAgent is not present?	*#True #False #0: No *#1: Yes (refreshed on use)	Machine
pid_ts_delay_app_launch_timeout_secs				
Time-out, in secs, for delaying of application launch. *Notes:* *1. This policy should be set on the remote AccessAgent (such as on the Citrix server).* *2. Effective only if pid_ts_delay_app_launch_enabled is enabled.* *3. Remote AccessAgent will, first, wait for connection to be established with local AccessAgent. If connection is not established within the time-out duration, application proceeds to launch.* *4. If local AccessAgent manages to establish connection with remote AccessAgent, remote AccessAgent will wait for another time-out period for automatic sign-on to be ready. If remote AccessAgent is not ready for automatic sign-on within the time-out duration, application proceeds to launch.* *5. Hence, user may potentially have to wait up to two times the time-out duration if local AccessAgent manages to establish connection with remote AccessAgent just before the first time-out duration lapses.*	[DO] "TSDelayAppLaunchTimeoutSecs"	Time-out, in seconds, for delaying of application launch	*10 (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_ts_aa_menu_option				
Whether to display menu options on AccessAgent user interface in a Terminal Server or Citrix session. *Notes:* *1. If policy value is 1, only "Remote session information" is displayed when there is local AccessAgent session. Full menu options are displayed when there is no local AccessAgent session. Same applies to right-click menu options for AccessAgent icon at Windows notification area.* *2. If policy value is 2, all menu options are displayed except for "Lock this computer" when there is local AccessAgent session. Full menu options are displayed when there is no local AccessAgent session. Same applies to right-click menu options for AccessAgent icon at Windows notification area. This option is recommended for Roaming Desktop configuration.*	[DO] "TSAaMenuOption"	Option for displaying menu options on remote AccessAgent	*#1: Display menu options only if there is no local AccessAgent session #2: Always display all menu o	Machine
pid_com_redir_enabled				
Whether the device monitoring mechanism should perform COM port redirection from the client machine (connecting to the Terminal Server) to the Terminal Server. *Note:* *If enabled for AA on Terminal Server or Citrix server, authentication devices on remote client machines (e.g., for thin clients where there is no AA installed) can be monitored. AA would map a virtual COM port (pid_com_redir_local_virtual_port) on the Terminal Server or Citrix server to a physical COM port (pid_com_redir_remote_physical_port) on the remote client.*	[DO] "ComRedirEnabled"	Enable COM port redirection?	#True *#False *#0: No #1: Yes (refreshed on startup)	Machine
pid_com_redir_local_virtual_port				
Virtual COM port on the Terminal Server to which data from the client COM port will get redirected to. *Note:* *Effective only if pid_com_redir_enabled is 1.*	[DO] "ComRedirLocalVirtualPort"	Virtual COM port on Terminal Server	*1 (refreshed on startup) (from 1 to 8)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_com_redir_remote_physical_port				
Physical COM port on the client to which the authentication device (e.g., RFID reader) is connected to. The redirection will take place from this port to the Terminal Server's virtual COM port. *Note:* *Effective only if pid_com_redir_enabled is 1.*	[DO] "ComRedirRemotePhysicalPort"	Physical COM port on client machine	*1 (refreshed on startup) (min 1)	Machine
Logon/Logoff policies				
pid_en_network_provider_enabled				
Whether to enable the Encentuate Network Provider (EnNetworkProvider). *Notes:* *1. Effective only if EnNetworkProvider has been installed by AccessAgent installer.* *2. If enabled, AccessAgent will attempt to automatically log on to itself using the credentials provided at Microsoft GINA. It works in conjunction with the AD password synchronization feature so that the same password can be used to log on to Windows as well as AccessAgent.*	[DO] "EnNetworkProviderEnabled"	Enable Encentuate Network Provider?	#True *#False *#0: No #1: Yes (refreshed on use)	Machine
pid_script_logon_enabled				
Whether to enable running of logon script during user logon.		Enable logon script during user logon?	#True *#False (refreshed on sync)	User
pid_script_logon_type				
Type of logon script to be run. *Note: Effective only if script logon is enabled.*		Logon script type	*#1: Batch #2: VBScript (refreshed on sync)	User
pid_script_logon_code				
Source code of logon script to be run. *Note: Effective only if script logon is enabled.*		Logon script code	(refreshed on sync)	User

Description	Registry	IMS Entry	Values	Scope
pid_logon_user_name_prefill_option				
Option for pre-filling Encentuate Logon prompt with a user name. *Notes:* *1. Policy should be set to 0 for shared desktops with many users.* *2. Policy should be set to 1 for personal desktops or shared desktops with very few users.* *3. Policy should be set to 2 for Terminal Server or Citrix Server. For policy value 2 to work properly, the following Microsoft registry value must be set to 0:* *[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system]"dontdisplaylastusername"*	[DO] "LogonUserNamePrefillOption"	Encentuate user name pre-fill option	#0: Do not pre-fill *#1: Pre-fill with last logged on user name #2: Pre-fill with currently logged on Windows user name (refreshed on use)	Machine
pid_logon_user_name_display_option				
Option for displaying the name of the currently logged on user. *Notes:* *1. If this policy is set to 2 or 3, AccessAgent displays the full name of the user, obtained from Active Directory upon logon to Wallet. Hence, the machine will have to be logged on to domain. If AccessAgent fails to obtain the full name from Active Directory, it will fallback to displaying the Encentuate user name.* *2. Due to the limited size of the UI, there is only enough space to display about 20 characters. If the name is truncated, it will be appended with "…".* *3. This policy affects all parts of the AccessAgent UI where user name is displayed, for example, main UI, locked screen.* *4. In a 2-factor deployment (RFID, USB, etc.), user does not need to enter user name to log on to AccessAgent. But if user forgets 2nd factor, user must enter user name and password to log on to AccessAgent or AccessAssistant. If the full name is always displayed, user may forget the logon user name easily as they do not need to use it every day and also do not see it in the AccessAgent UI. Hence, as a best practice, policy value 1 should be used for a 2-factor deployment.*	[DO] "LogonUserNameDisplayOption"	Encentuate user name display option	*#1: Encentuate user name #2: First name followed by last name #3: Last name followed by first name (refreshed on logon)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_script_logoff_enabled				
Whether to enable running of logoff script during user logoff.		Enable logoff script during user logoff?	#True *#False (refreshed on sync)	User
pid_script_logoff_type				
Type of logoff script to be run. *Note: Effective only if script logoff is enabled.*		Logoff script type	*#1: Batch #2: VBScript (refreshed on sync)	User
pid_script_logoff_code				
Source code of logoff script to be run. *Note: Effective only if script logoff is enabled.*		Logoff script code	(refreshed on sync)	User
pid_logoff_manual_enabled				
Whether to allow user to manually log off AccessAgent. *Note:* *If this policy is disabled, the "Log off AccessAgent" option will not appear in any part of AccessAgent UI.*	[DO] "LogoffManualEnabled"	Allow user to manually log off AccessAgent?	#0: No *#1: Yes *#True #False (refreshed on sync)	Machine User
✱ **pid_logoff_manual_action**				
Actions to be performed by AccessAgent on manual logoff by user. *Notes:* *1. Effective when user manually logs off Wallet from desktop or transparent screen lock.* *2. If pid_lusm_sessions_max > 1, AccessAgent with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.* *This is the recommended policy value for Local User Session Management. If policy value is 2, AccessAgent will be logged off, but user will not be able to re-log on to AccessAgent unless Ctrl-Alt-Del is pressed to log on from the Encentuate-replaced Windows security dialog.*	[DO] "LogoffManualAction"	Actions on manual logoff by user	#1: Log off Windows *#2: Log off Wallet #4: Log off Wallet and lock computer (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User

Description	Registry	IMS Entry	Values	Scope
pid_logoff_manual_action_countdown_secs				
Confirmation countdown duration, in seconds, for manual logoff by user. *Notes:* *1. Effective when user manually logs off Wallet from desktop or locked computer window.* *2. If policy value is non-zero, user has to click on the prompt to confirm logoff. If user does not confirm, AccessAgent will not proceed with the logoff.*	[DO] "LogoffManualActionCountdownSecs"	Confirmation countdown duration, in seconds, for manual logoff by user	*30 (0 to disable confirmation countdown) (refreshed on sync for user policy) (refreshed on use for machine policy)	Machine User
pid_wallet_logoff_action_for_apps_default				
Default action to take for all applications when user logs off AccessAgent. *Notes:* *1. If policy value is 1, AccessAgent will attempt to log off all instances of applications. The AccessProfile for each application must contain a logoff action, otherwise the application logoff will not be performed.* *2. If policy value is 2, AccessAgent will close all instances of applications that are monitored by AccessAgent. All applications that have AccessProfiles are monitored, regardless of whether AccessAgent is used to log on to the application.* *3. This policy is effective whenever a user is logged off from AccessAgent, for example, during a switch user operation.*		Default action for applications, when user logs off AccessAgent	#1: Log off the application #2: Close the application *#3: Do nothing (refreshed on sync)	System
pid_logoff_app_timeout_secs				
Time-out, in secs, for logging off applications. *Notes:* *1. When AccessAgent logs off a Wallet (during manual logoff or switch user), logging off of applications may occur (depends on configuration). This policy specifies a configurable time-out for logging off applications.* *2. If an application is not successfully terminated by its AccessProfile after the time-out, it can be forced to terminate by setting the "Terminate on time-out" and "Time-out" attributes of the "gen_sign_out_trigger" appropriately.*	[DO] "LogoffAppTimeoutSecs"	Time-out, in seconds, for application logoff	*5 (from 0 to 60) (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
Encentuate Hot Key policies				
pid_enc_hot_key_enabled				
Whether Encentuate Hot Key is enabled. *Notes:* *1. At EnGINA, Hot Key brings user to logon screen.* *2. At locked screen, Hot Key brings user to unlock screen.* *3. At desktop, if AccessAgent is not logged on, Hot Key launches logon screen.* *4. At desktop, if AccessAgent is logged on, Hot Key's behavior is defined by Encentuate Hot Key action.*	[DO] "EncHotKeyEnabled"	Enable Encentuate Hot Key?	*#1: Yes #0: No *#True #False (refreshed on startup)	Machine System
pid_enc_hot_key_sequence				
The Encentuate Hot Key sequence. *Note:* *Effective only if Encentuate Hot Key is enabled.*	[DO] "EncHotKeySequence"	Encentuate Hot Key sequence	*#Ctrl *#Alt *#E (max 3 keys from set of: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E) (2 of the keys in this set should be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt) (refreshed on startup)	Machine System
pid_enc_hot_key_action_countdown_secs				
Confirmation countdown duration, in seconds, for pressing Encentuate Hot Key. *Notes:* *1. Effective only if Encentuate Hot Key is enabled.* *2. Effective only if Encentuate Hot Key is pressed while AccessAgent is logged on and computer is not locked.*	[DO] "EncHotKeyActionCountdownSecs"	Confirmation countdown duration, in seconds, for pressing Encentuate Hot Key	*5 (0 to disable confirmation countdown) (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System

Description	Registry	IMS Entry	Values	Scope
pid_enc_hot_key_action				
Actions to be performed by AccessAgent if Encentuate Hot Key is pressed at desktop while AccessAgent is logged on. *Notes:* *1. Effective only if Encentuate Hot Key is enabled.* *2. Actions taken only if Hot Key is pressed at desktop while AccessAgent is logged on.* *3. If pid_lusm_sessions_max > 1, AA with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.*	[DO] "EncHotKeyAction"	Encentuate Hot Key press actions at desktop when AccessAgent is logged on	#0: No action #1: Log off Windows #2: Log off Wallet #4: Lock computer #5: Log off Wallet and lock computer *#9: Launch AccessAgent window (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System
pid_enc_hot_key_not_logged_on_action				
Actions to be performed by AccessAgent if Encentuate Hot Key is pressed at desktop while AccessAgent is not logged on. *Notes:* *1. Effective only if pid_enc_hot_key_enabled is enabled.* *2. Actions taken only if Hot Key is pressed at desktop while AccessAgent is not logged on.* *3. If pid_lusm_sessions_max > 1, AccessAgent with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.* *However, if the desktop is the default desktop, whether it can be logged off is determined by pid_lusm_default_desktop_preserved_enabled.*	[DO] "EncHotKeyNotLoggedOnAction"	Encentuate Hot Key press actions at desktop when AccessAgent is not logged on	#0: No action #1: Log off Windows #4: Lock computer *#9: Launch AccessAgent window (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System

Description	Registry	IMS Entry	Values	Scope
Emergency Hot Key policies				
pid_emergency_hot_key_enabled				
Whether Emergency Hot Key is enabled. *Notes:* *1. If user presses this Hot Key at computer locked screen, AccessAgent unlocks computer without any credentials but will log off AccessAgent, if logged on.* *2. To use the Emergency Hot Key, unlock option must be set to 3.* *3. Use of the Emergency Hot Key should be subject to proper behavior of auto-logoff from applications.* *4. Use of the Emergency Hot Key should be subject to proper behavior of auto-logoff from applications.*	[DO] "EmergencyHotKeyEnabled"	Enable Emergency Hot Key?	#1: Yes *#0: No #True *#False (refreshed on startup)	Machine System
pid_emergency_hot_key_sequence				
The Emergency Hot Key sequence. *Note:* *Effective only if Emergency Hot Key is enabled.*	[DO] "EmergencyHotKeySequence"	Emergency Hot Key sequence	*#Ctrl *#Alt *#End (max 3 keys from set of: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E) (2 of the keys in this set should be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt) (refreshed on startup)	Machine System
Presence detector policies				
pid_presence_detector_enabled				
Whether presence detector is enabled. *Note:* *This policy does not automatically enabled or disable the third-party presence detector hardware and software.*	[DO] "PresenceDetectorEnabled"	Enable presence detector?	#1: Yes *#0: No #True *#False (refreshed on startup)	Machine System

Description	Registry	IMS Entry	Values	Scope
pid_presence_detector_walk_away_key_sequence				
The key sequence that the presence detector will send when a user walks away from it. *Notes:* *1. Effective only if pid_presence_detector_enabled is enabled.* *2. The same key sequence should be configured on the presence detector by using third-party software. For RF IDeas pcProx-Sonar, configure the "Walk-away Keystrokes" using the pcProx-Sonar Configuration Utility.*	[DO] "PresenceDetectorWalkAwayKeySequence"	Key sequence sent by presence detector when user walks away	*#Ctrl *#Alt *#PgDn (max 3 keys from set of: Ctrl, Shift, Alt, Ins, Del, Home, End, PgUp, PgDn, Break, E) (2 of the keys in this set should be used so that the probability of conflict with other applications is minimized: Ctrl, Shift, Alt) (refreshed on startup)	Machine System
pid_presence_detector_walk_away_action				
Actions to be performed by AccessAgent when presence detector detects a user walking away while no user is logged on. *Notes:* *1. Effective only if pid_presence_detector_enabled is enabled.* *2. Currently, this is supported only if pid_lusm_sessions_max = 1. In future, if pid_lusm_sessions_max > 1, AccessAgent with policy value 1 (Log off Windows) will log off the user's desktop session and show the computer locked screen.*	[DO] "PresenceDetectorWalkAwayAction"	Actions performed by AccessAgent when presence detector detects user walking away while no user is logged on	#0: No action #1: Log off Windows #2: Log off Wallet *#4: Lock computer #5: Log off Wallet and lock computer (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System
pid_presence_detector_walk_away_action_countdown_secs				
Confirmation countdown duration, in seconds, when presence detector detects a user walking away. *Note:* *Effective only if pid_presence_detector_enabled is enabled.*	[DO] "PresenceDetectorWalkAwayActionCountdownSecs"	Confirmation countdown duration, in seconds, when presence detector detects user walking away	*5 (0 to disable confirmation countdown) (refreshed on sync for system policy) (refreshed on use for machine policy)	Machine System

Description	Registry	IMS Entry	Values	Scope

Configurable text policies

EnGINA text policies

pid_engina_welcome_text

Description	Registry	IMS Entry	Values	Scope
Configurable text for EnGINA welcome message. *Notes:* *1. This message will be displayed, followed by a blank line, and then messages in one of the configurable text policies below (depending on second factors supported list).* *2. Consecutive strings are separated by a blank line.* *3. "\n\n" can be added if more blank lines are desired.*		Welcome message (Maximum 2 lines)	*#This computer is protected by Encentuate AccessAgent. *#If you are here for the first time, click 'Sign up' to get started. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

pid_engina_logon_with_pwd_text

Description	Registry	IMS Entry	Values	Scope
Configurable text for password logon. *Note: See pid_engina_welcome_text.*		Instructions for password logon (Maximum 2 lines)	*#To log on, click 'Log on' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

pid_engina_logon_with_rfid_text

Description	Registry	IMS Entry	Values	Scope
Configurable text for RFID logon. *Note: See pid_engina_welcome_text.*		Instructions for RFID logon (Maximum 2 lines)	*#To log on, tap your RFID card. *#If you do not have your RFID card, click 'Log on' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_engina_logon_with_usb_key_text				
Configurable text for USB Key logon. *Note: See pid_engina_welcome_text.*		Instructions for USB Key logon (Maximum 2 lines)	*#To log on, insert your Encentuate USB Key into the USB port now. If you have already inserted your Key and are not prompted for password, remove your Key and insert it back again, or press Ctrl-Alt-Del. *#If you do not have your Encentuate USB Key, click 'Log on' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_engina_logon_with_arfid_text				
Configurable text for active proximity badge logon. *Note: See pid_engina_welcome_text.*		Instructions for active proximity badge logon (Maximum 2 lines)	*#To log on, present your active proximity badge. *#To log on without active proximity badge, click 'Log on' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_engina_logon_with_fingerprint_text				
Configurable text for fingerprint logon. *Note: See pid_engina_welcome_text.*		Instructions for fingerprint logon (Maximum 2 lines)	*#To log on, place your registered finger on the sensor. *#To log on without fingerprint, click 'Log on' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_engina_logon_with_fingerprint_or_rfid_text				
Configurable text for fingerprint or RFID logon. *Note: See pid_engina_welcome_text.*		Instructions for fingerprint or RFID logon (Maximum 2 lines)	*#To log on, place your registered finger on the sensor or tap your RFID card. *#To log on without fingerprint or RFID card, click 'Log on' or press Ctrl-Alt-Del. (2 strings max) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_logon_credentials_text				
Configurable text that is to be displayed right above the logon credentials when user clicks on 'Log on'. *Note:* *If pid_enc_pwd_is_ad_pwd_enabled is set to True, this policy should be modified accordingly, for example, "Enter your Windows domain user name and password to log on."*		Logon credentials message (Maximum 1 line)	*#Enter your user name and password to log on. (1 string max.) (text box takes 2 lines max, about 40 chars per line) (refreshed on sync)	System
Unlock text policies				
pid_unlock_text				
Configurable text for computer locked message. *Notes:* *1. This message will be displayed, followed by a blank line, and then messages in one of the configurable text policies below (depending on current Wallet and pid_unlock option).* *2. Consecutive strings are separated by a blank line.* *3. "\n\n" can be added if more blank lines are desired.*		Locked computer message (Maximum 1 line)	*#This computer is protected by Encentuate AccessAgent, and has been locked. (1 string max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_pwd_option_1_text				
Configurable text for unlocking with password when computer locked and pid_unlock option is 1. *Note: See pid_unlock text.*		Instructions for unlocking with password when unlock policy is ‘only the same user can unlock’ (Maximum 2 lines)	*#To unlock, click ‘Unlock this computer’ or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_pwd_option_3_text				
Configurable text for unlocking with password when computer locked and pid_unlock option is 3. *Note: See pid_unlock text.*		Instructions for unlocking with password when unlock policy is ‘any user with or without current desktop account in Wallet can unlock’ (Maximum 2 lines)	*#To unlock, click ‘Unlock this computer’ or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_pwd_option_4_text				
Configurable text for unlocking with password when computer locked and pid_unlock_option is 4. *Note: See pid_unlock_text.*		Instructions for unlocking with password when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (textbox takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_usb_key_option_1_text				
Configurable text for unlocking with USB Key when computer locked and pid_unlock option is 1. *Note: See pid_unlock text.*		Instructions for unlocking with USB Key when unlock policy is 'only the same user can unlock' (Maximum 2 lines)	*#To unlock, insert your Encentuate USB Key into the USB port now. If you have already inserted your Key and are not prompted for password, remove your Key and insert it back again, or press Ctrl-Alt-Del. *#If you do not have your Encentuate USB Key, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_usb_key_option_3_text				
Configurable text for unlocking with USB Key when computer locked and pid_unlock_option is 3. *Note: See pid_unlock text.*		Instructions for unlocking with USB Key when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)	*#To unlock, insert your Encentuate USB Key into the USB port now. If you have already inserted your Key and are not prompted for password, remove your Key and insert it back again, or press Ctrl-Alt-Del. *#If you do not have your Encentuate USB Key, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_usb_key_option_4_text				
Configurable text for unlocking with USB Key when computer locked and pid_unlock option is 4. *Note: See pid_unlock text.*		Instructions for unlocking with USB Key when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, insert your Encentuate USB Key into the USB port now. If you have already inserted your Key and are not prompted for password, remove your Key and insert it back again, or press Ctrl-Alt-Del. *#If you do not have your Encentuate USB Key, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (textbox takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_rfid_option_1_text				
Configurable text for unlocking with RFID when computer locked and pid_unlock option is 1. *Note: See pid_unlock text.*		Instructions for unlocking with RFID when unlock policy is ‘only the same user can unlock’ (Maximum 2 lines)	*#To unlock, tap your RFID card. *#If you do not have your RFID card, click ‘Unlock this computer’ or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_rfid_option_3_text				
Configurable text for unlocking with RFID when computer locked and pid_unlock_option is 3. *Note: See pid_unlock text.*		Instructions for unlocking with RFID when unlock policy is ‘any user with or without current desktop account in Wallet can unlock’ (Maximum 2 lines)	*#To unlock, tap your RFID card. *#If you do not have your RFID card, click ‘Unlock this computer’ or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_rfid_option_4_text				
Configurable text for unlocking with RFID when computer locked and pid_unlock_option is 4. *Note: See pid_unlock text.*		Instructions for unlocking with RFID when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, tap your RFID card. *#If you do not have your RFID card, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (textbox takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_arfid_option_1_text				
Configurable text for unlocking with active proximity badge when computer locked and pid_unlock_option is 1. *Note: See pid_unlock text.*		Instructions for unlocking with active proximity badge when unlock policy is 'only the same user can unlock' (Maximum 2 lines)	*#To unlock, present your active proximity badge. *#To unlock without active proximity badge, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_arfid_option_3_text				
Configurable text for unlocking with active proximity badge when computer locked and unlock option is 3. *Note: See pid_unlock text.*		Instructions for unlocking with active proximity badge when unlock policy is 'any user with or without current desktop account in Wallet can unlock' (Maximum 2 lines)	*#To unlock, present your active proximity badge. *#To unlock without active proximity badge, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_arfid_option_4_text				
Configurable text for unlocking with active proximity badge when computer locked and pid_unlock_option is 4. *Note: See pid_unlock text.*		Instructions for unlocking with active proximity badge when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, present your active proximity badge. *#To unlock without active proximity badge, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (textbox takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_fingerprint_option_1_text				
Configurable text for unlocking with fingerprint when computer locked and unlock option is 1. *Note: See pid_unlock_text.*		Instructions for unlocking with fingerprint when unlock policy is ‘only the same user can unlock’ (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor. *#To unlock without fingerprint, click ‘Unlock this computer’ or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_fingerprint_option_3_text				
Configurable text for unlocking with fingerprint when computer locked and unlock option is 3. *Note: See pid_unlock_text.*		Instructions for unlocking with fingerprint when unlock policy is ‘any user with or without current desktop account in Wallet can unlock’ (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor. *#To unlock without fingerprint, click ‘Unlock this computer’ or press Ctrl-Alt-Del. (2 strings max.) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_fingerprint_option_4_text				
Configurable text for unlocking with fingerprint when computer locked and pid_unlock_option is 4. *Note: See pid_unlock_text.*		Instructions for unlocking with fingerprint when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor. *#To unlock without fingerprint, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (textbox takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_fingerprint_or_rfid_option_1_text				
Configurable text for unlocking with fingerprint or RFID when computer locked and pid_unlock_option is 1. *Note: See pid_unlock_text.*		Instructions for unlocking with fingerprint or RFID when unlock policy is ‘only the same user can unlock’ (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor or tap your RFID card. *#To unlock without fingerprint or RFID card, click ‘Unlock this computer’ or press Ctrl-Alt-Del. (2 strings max) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_with_fingerprint_or_rfid_option_3_text				
Configurable text for unlocking with fingerprint or RFID when computer locked and pid_unlock_option is 3. *Note: See pid_unlock_text.*		Instructions for unlocking with fingerprint or RFID when unlock policy is ‘any user with or without current desktop account in Wallet can unlock’ (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor or tap your RFID card. *#To unlock without fingerprint or RFID card, click ‘Unlock this computer’ or press Ctrl-Alt-Del. (2 strings max) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_unlock_with_fingerprint_or_rfid_option_4_text				
Configurable text for unlocking with fingerprint or RFID when computer locked and pid_unlock_option is 4. *Note: See pid_unlock_text.*		Instructions for unlocking with fingerprint or RFID when unlock policy is 'only the same user can unlock, but different user can re-log on to Windows' (Maximum 2 lines)	*#To unlock, place your registered finger on the sensor or tap your RFID card. *#To unlock without fingerprint or RFID card, click 'Unlock this computer' or press Ctrl-Alt-Del. (2 strings max) (text box takes 15 lines max, about 40 chars per line) (refreshed on sync)	System
pid_unlock_credentials_text				
Configurable text that is to be displayed right above the unlock credentials when user clicks on 'Unlock this computer'. *Note: If Encentuate password is AD password is set to True, this policy should be modified accordingly, for example, "Enter your Windows domain user name and password to unlock."*		Unlock credentials message (Maximum 1 line)	*#Enter your user name and password to unlock. (1 string max.) (text box takes 2 lines max, about 40 chars per line) (refreshed on sync)	System
RFID text policies				
pid_rfid_name_text				
Configurable text for RFID name, for example, 'RFID card'.		RFID name	*RFID card (refreshed on sync)	System
Sign up text policies				
pid_bind_display_template				
The template to be used for displaying the sign-up dialog. *Notes:* *1. The Domain field is also shown if and only if the enterprise directory is AD.* *2. Other than the domain, the template can only support either 1 or 2 fields. To display only one field, set the Label of one of the fields to a blank entry. The field with the blank Label will not be displayed.*		Template for sign-up dialogBind template*	#Enter your domain user name and password for identity verification. *#User name *#Password (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
AccessAssistant and Web Workplace text policies				
pid_accessanywhere_otp_reset_link_text				
Configurable text for the OTP (OATH) reset link on AccessAssistant and Web Workplace. *Note: Effective only if pid_auth_authentication_option for "AccessAnywhere" contains "OTP (OATH)".*		Text for the OTP (OATH) reset link on AccessAssistant and Web Workplace.	*Reset OTP token (refreshed on sync)	System
Authentication Service policies				
Password policies				
pid_auth_reauth_with_enc_pwd_enabled				
Whether Encentuate password re-authentication is required before performing automatic sign-on for the authentication service. *Note: Effective only if "authentication is enterprise" is enabled for the authentication service.*		Require re-authentication before performing automatic sign-on?	#True *#False (refreshed on sync)	System
pid_auth_pwd_is_ad_pwd				
Whether the authentication service is displayed as a Windows user account in AccessAdmin.		Is the password the Windows logon password?	#True *#False (refreshed on use)	System
pid_auth_fortification_pwd_min_length				
Minimum length of an acceptable password for the authentication service. *Note: Effective if pid_auth_fortification_random_pwd_ enabled is enabled.*		Minimum password length	*6 (from 1 to 99) (refreshed on sync)	System
pid_auth_fortification_pwd_max_length				
Maximum length of an acceptable password for the authentication service. *Note: Effective if pid_auth_fortification_random_pwd_ enabled is enabled.*		Maximum password length	*20 (from 1 to 99) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_auth_fortification_pwd_min_numerics_length				
Minimum number of numeric characters for an acceptable password for the authentication service. *Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.*		Minimum number of numeric characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_auth_fortification_pwd_min_alphabets_length				
Minimum number of alphabetic characters for an acceptable password for the authentication service. *Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.*		Minimum number of alphabetic characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_auth_fortification_pwd_min_special_chars_length				
Minimum number of special characters for an acceptable password for the authentication service. *Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.*		Minimum number of special characters	*0 (from 0 to 99) (refreshed on sync)	System
pid_auth_fortification_pwd_max_numerics_length				
Maximum number of numeric characters for an acceptable password for the authentication service. *Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.*		Maximum number of numeric characters	*10 (from 0 to 99) (0 for no max limit) (refreshed on sync)	System
pid_auth_fortification_pwd_max_alphabets_length				
Maximum number of alphabetic characters for an acceptable password for the authentication service. *Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.*		Maximum number of alphabetic characters	*10 (from 0 to 99) (0 for no max limit) (refreshed on sync)	System
pid_auth_fortification_max_special_chars_length				
Maximum number of special characters for an acceptable password for the authentication service. *Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.*		Maximum number of special characters	*10 (from 0 to 99) (0 for no max limit) (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_auth_fortification_pwd_mixed_case_enforced				
Whether to enforce the use of both upper case and lower case characters for the password of the authentication service. *Note: Effective if pid_auth_fortification_random_pwd_enabled is enabled.*		Enforce the use of both upper case and lower case characters?	#True *#False (refreshed on sync)	System
pid_auth_fortification_random_pwd_enabled				
Whether manual password change with random password is enabled for the authentication service.		Enable manual password change with random password?	#True *#False (refreshed on sync)	User
Authentication policies				
pid_auth_is_enterprise				
Whether an authentication service is an enterprise authentication service.		Is it an enterprise authentication service?	#True *#False (refreshed on sync)	System
pid_auth_inject_pwd_entry_option_default				
Default automatic sign-on password entry option for the authentication service. *Notes:* *1. Effective only if "authentication is enterprise" is enabled for the authentication service.* *2. Overrides Wallet inject password entry option default.*		Default automatic sign-on password entry option for the authentication service	#1: Automatic logon *#2: Always #3: Ask #4: Never #5: Certificate #6: Use application settings (refreshed on sync)	System
pid_auth_sso_enabled				
Whether to enable automatic sign-on for the authentication service. *Note: Effective only if "authentication is enterprise" is enabled for the authentication service.*		Enable automatic sign-on?	*#True #False (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
✱ pid_auth_authentication_option				
Option to control what authentication modes AccessAgent should support for the authentication service. *Note: Effective only if "authentication is enterprise" is enabled for the authentication service.*		Authentication modes to be supported	*#1: Password #2: SCR #4: CAPI #8: OTP #16: MAC #32: CCOW (multiple allowed) (refreshed on sync)	System
pid_auth_accounts_max				
Maximum number of accounts that user can store for the authentication service. *Notes:* *1. When the number of accounts has reached or exceeded the maximum specified by this policy:* *a) AccessAgent does not capture anymore new accounts for this authentication service.* *b) If user clicks on "Add new user" button in Wallet Manager, AccessAgent prompts that the number of accounts has reached the limit.* *2. User policy, if defined, overrides system policy.*		Maximum number of accounts allowed for the authentication service	*0 (from 0 to 10) (0 for no max limit) (refreshed on sync)	User System
pid_auth_capture_prompt_enabled				
Whether user should be prompted during auto-capture of password for the authentication service. *Notes:* *1. Effective only if pid_auth_is_enterprise is enabled for the authentication service.* *2. In the case of policy value False, if some user is already logged on and another user wants to use the computer for some time, the second user's application passwords may be auto-captured into the first user's Wallet. Hence, if pid_auth_capture_prompt_enabled is set to False for an authentication service, it is recommended that pid_auth_account_max be set to 1 for the same authentication service.*		Prompt user on auto-capture of password?	*#True #False (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
User-defined policies				
pid_auth_inject_pwd_entry_option				
Password entry of injection policy per authentication service.			#1: Automatic logon *#2: Always #3: Ask #4: Never #5: Certificate #6: Use application settings (refreshed on use)	User
pid_auth_inject_user_default				
Default user of injection policy per authentication service.			(refreshed on use)	User
Application policies				
pid_app_authentication_option				
Option to control what authentication modes AccessAgent should support for the application.		Authentication modes to be supported	*#1: Password #2: SCR #4: CAPI #8: OTP #16: MAC (multiple allowed) (refreshed on sync)	System
pid_app_reauth_with_enc_pwd_enabled				
Whether Encentuate password re-authentication is required before performing automatic sign-on for the application. *Note: Overrides authenticate/re-authenticate with Encentuate password.*		Require re-authentication before performing automatic sign-on?	#True *#False (refreshed on sync)	System
pid_app_inject_pwd_entry_option_default				
Default automatic sign-on password entry option for the application. *Note: Overrides authentication inject password entry option default and Wallet inject password entry option default.*		Default automatic sign-on password entry option for the application	#1: Automatic logon *#2: Always #3: Ask #4: Never #5: Certificate #6: Use application settings (refreshed on sync)	System

Description	Registry	IMS Entry	Values	Scope
pid_app_wallet_logoff_action				
Action to take for the application when user logs off AccessAgent. *Notes:* *1. This policy overrides Wallet logoff action for applications default.* *2. See the notes for Wallet logoff action for applications default.* *3. For web applications, each URL is considered an application. Internet Explorer (IE) is also considered an application. In this context, the web application policy overrides the IE policy, which overrides Wallet logoff action for applications default.* *4. Recommended settings for IE and Windows Explorer: 2 and 3 respectively.* *5. This policy is set to 3 for Windows logon (application GINA) when IMS is installed.*		Action for the application, when user logs off AccessAgent	#1: Log off the application #2: Close the application *#3: Do nothing (refreshed on sync)	System
User-defined policies				
pid_app_auth_inject_pwd_entry_option				
Password entry of injection policy per application per authentication service.			#1: Automatic logon *#2: Always #3: Ask #4: Never #5: Certificate #6: Use application settings (refreshed on use)	User
pid_app_auth_inject_user_default				
Default user of injection policy per application per authentication service.			(refreshed on use)	User
Troubleshooting				
pid_wallet_sync_manual_enabled				
Whether to enable a “Synchronize with IMS” option by right-clicking AA in WNA.	[T] “WalletSyncManualEnabled”		*#0: No #1: Yes (refreshed on use)	Machine

Description	Registry	IMS Entry	Values	Scope
pid_wallet_delete_enabled				
Whether to enable a "Delete user Wallets" option by right-clicking AA in WNA. *Notes:* *1. This menu item is only available when no user is logged on to AA.* *2. This menu item deletes all user Wallets, but not the machine Wallet.* *3. If this feature is to be used on a Citrix or Terminal Server or a workstation with Local User Session Management (LUSM) enabled, make sure that only one desktop session is running while deleting the Wallets. If multiple sessions are running, the behavior of AA in other sessions after deleting the Wallets is unpredictable.*	[T] "WalletDeleteEnabled"		*#0: No #1: Yes (refreshed on use)	Machine
pid_machine_policy_override_enabled				
Whether to override machine policies using registry values. *Notes:* *1. If enabled, machine policies can be overridden for this machine by specifying their values in the registry key [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\DeploymentOptions]. E.g., pid_second_factors_supported_list can be specified using the registry value "SecondFactorsSupportedList".* *2. This temporary policy is useful for troubleshooting, especially if there is no administrator access to IMS Server. Remember to disable this policy after testing is completed, so that the machine can continue to be managed through AccessAdmin.*	[T] "MachinePolicyOverrideEnabled		*#0: No #1: Yes (refreshed on use)	Machine

Using The IMS Configuration Utility

This appendix contains reference information about all of the configuration directives that are included in the Encentuate IMS Server's configuration file (ims.xml). Manipulating the configuration file using the IMS Configuration Utility allows you to control the behavior of Encentuate IMS Server.

The IMS Server configuration file is different for every organization. The configuration is pre-determined before full deployment takes place.

Configuration information specific to the IMS Server is stored either in the database or in an Extensible Markup Language (XML) based configuration file. The deciding factor is based on whether the configuration data is required to enforce data integrity in the database.

For most deployments, the configuration file is called ims.xml and can be found in the config subdirectory of Encentuate IMS Server's main installation directory (imsserver\ims\config\ims.xml). The configuration data in the configuration file is tightly bound to the configuration data in the database. It is important to analyze the dependencies before making any modifications.

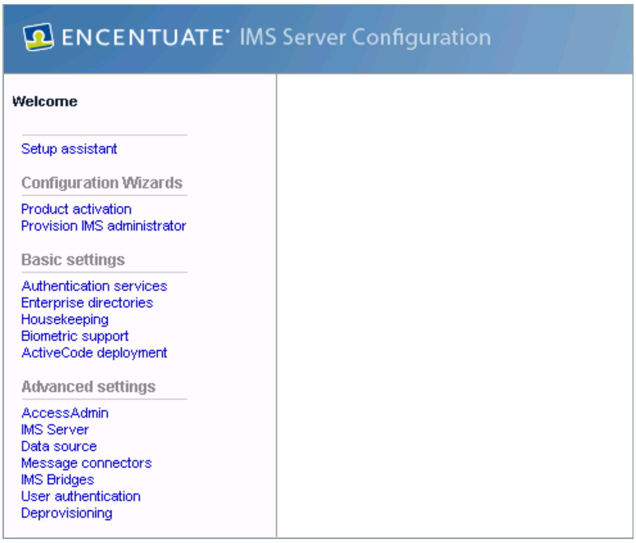
The IMS Configuration Utility can be configured such that it can be accessed by a set of IPs. However, only the local computer's IP is added to the configuration file by default. The file is imsserver\conf\server.xml

When adding IPs, add them separated by commas where the IP is. Look for the line in the file that looks like:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="127.0.0.1,$IP$"/>
```

Accessing the IMS Configuration Utility

The IMS Configuration Utility is installed, by default, on port 8080 and can only be accessed locally from the server console, for security reasons (URL: http://imsserver:8080/). It can be accessed from the Windows Start menu through *Start >> Programs >> Encentuate IMS Server >> IMS Configuration Utility.* Unlike AccessAdmin, the utility does not authenticate users.



IMS Server Configuration

You can also access the IMS Configuration utility using Remote Desktop connection. Run the command: `mstsc /v imsserver.` When you are connected to the remote server, enter your Administrator user name and password to access the computer. Once you are connected, you can access the utility through the Windows Start menu.

IMS Configuration Utility is only accessible from the physical IMS server. If the server IP has changed since installation, you can access this page using http://localhost:8080.

After making any changes to the IMS Server using the Configuration Utility, the IMSService must be restarted for the changes to take effect.

Using the Setup Assistant

To use the Setup Assistant:

❶ Select **Setup Assistant** from the IMS Configuration Utility navigation panel. This displays the **Configure domains** start screen for the Active Directory configuration.

*The **Configure domains** screen will not be displayed if there is no domain configured in IMS. The user is taken directly to the **Add domain** screen instead.*

❷ Configure the Active Directory.

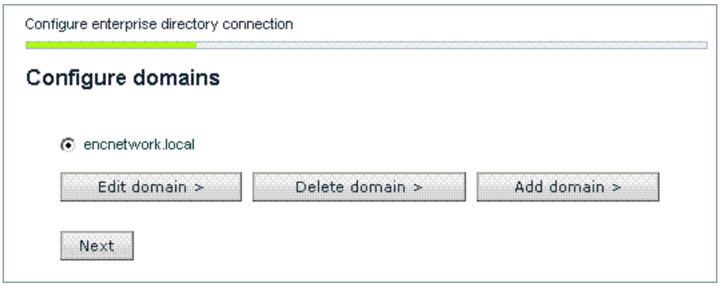
Configuring the Active Directory

You can configure your Active Directory as enterprise directory and assign valid domain user as Administrator using the **Setup Assistant** wizard.

To add a domain:

❶ Select *Configuration Wizards >> Active Directory* from the IMS Configuration Utility navigation panel. This displays the **Configure Domains** screen.

In the **Configure domains** screen, click **Add domain**.



Configure enterprise directory connection

Configure domains

◉ encnetwork.local

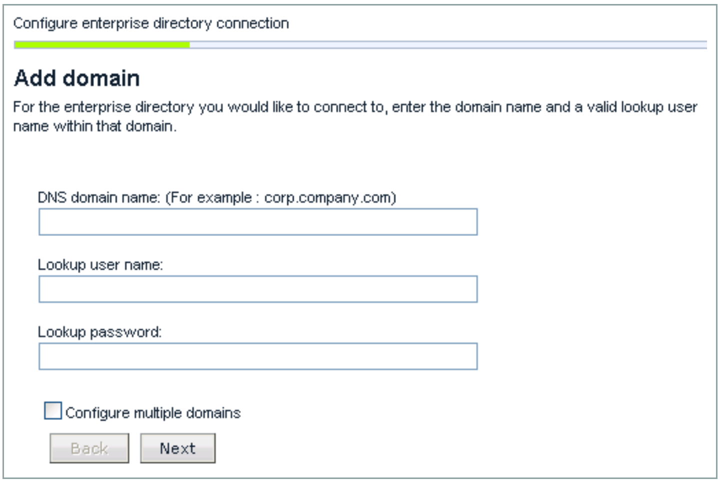
Configure domain

The **Add domain** fields are displayed.

❷ Enter information for the new domain.

DNS domain name
Enter the DNS Domain Name for the Active Directory. This is usually of the form test.company.com.

Lookup user name
Lookup password
Enter the lookup user name and password. This is a valid domain user but does not have to have Administrator rights. These credentials will be stored on the IMS Server to facilitate validation of user credentials and searching for users and their attributes. The password for this account should be set such that it does not expire.



Configure enterprise directory connection

Add domain

For the enterprise directory you would like to connect to, enter the domain name and a valid lookup user name within that domain.

DNS domain name: (For example : corp.company.com)

Lookup user name:

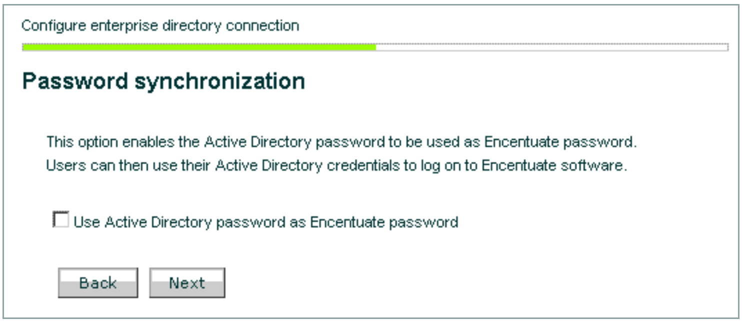
Lookup password:

□ Configure multiple domains

Enter the necessary information in their respective fields

After completing all the fields, click **Next**.

❸ The **Active Directory Configuration: Step 2 of 4: Password synchronization** is displayed.



Configure enterprise directory connection

Password synchronization

This option enables the Active Directory password to be used as Encentuate password.
Users can then use their Active Directory credentials to log on to Encentuate software.

□ Use Active Directory password as Encentuate password

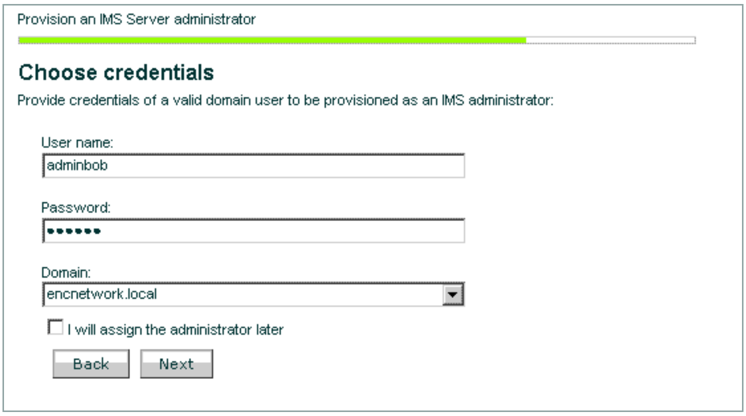
Mark the checkbox and click Next

Selecting **Use Active Directory password as Encentuate password** will allow users to use their Active Directory password as their Encentuate password.

This is only useful if AccessAgent will be deployed. If this is a MAC-only deployment, this option can be left un-selected. Click **Next**.

❺ The **Active Directory Configuration: Step 3 of 4: Choose credentials** screen is displayed.

Enter the user name, password and domain of a valid Active Directory user. This user will be provisioned on the IMS Server and automatically promoted to Administrator role. If you would like to skip this step, select **I will assign the Administrator later**.



Provision an IMS Server administrator

Choose credentials

Provide credentials of a valid domain user to be provisioned as an IMS administrator:

User name: adminbob

Password: ••••••

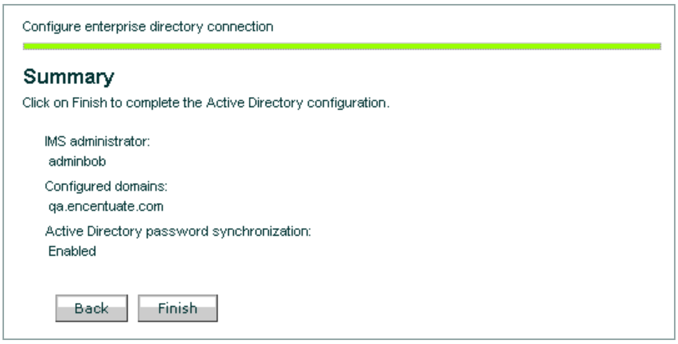
Domain: encnetwork.local

□ I will assign the administrator later

Enter the user credentials, then click Next

Click **Next**.

❻ The **Active Directory Configuration Wizard: Step 4 of 4: Summary** shows a summary of the configuration settings. After reviewing the settings, click **Finish**.



Configure enterprise directory connection

Summary

Click on Finish to complete the Active Directory configuration.

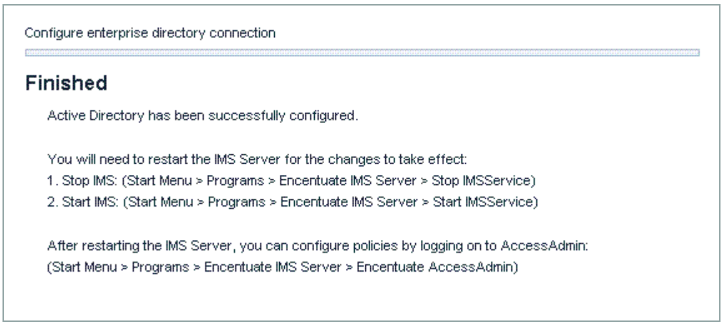
IMS administrator:
adminbob

Configured domains:
qa.encentuate.com

Active Directory password synchronization:
Enabled

Check the summary details and click Finish to proceed.

If the configuration settings are applied successfully, a summary screen will be shown:



Configure enterprise directory connection

Finished

Active Directory has been successfully configured.

You will need to restart the IMS Server for the changes to take effect:
1. Stop IMS: (Start Menu > Programs > Encentuate IMS Server > Stop IMSService)
2. Start IMS: (Start Menu > Programs > Encentuate IMS Server > Start IMSService)

After restarting the IMS Server, you can configure policies by logging on to AccessAdmin:
(Start Menu > Programs > Encentuate IMS Server > Encentuate AccessAdmin)

Summary screen indicating successful configuration

To modify an existing domain:

❶ Select *Configuration Wizards >> Active Directory* from the IMS Configuration Utility navigation panel.

❷ The Active Directory Configuration: Step 1 of 4: Configure Domains is displayed.

❸ Select the existing domain and click Edit Domain.

❹ Modify the values in the fields and click Next to apply changes.

To delete a domain:

❶ Select *Configuration Wizards >> Active Directory* from the IMS Configuration Utility navigation panel.

❷ The Active Directory Configuration: Step 1 of 4: Configure Domains is displayed.

❸ Select the existing domain and click Delete Domain.

Using the configuration wizards

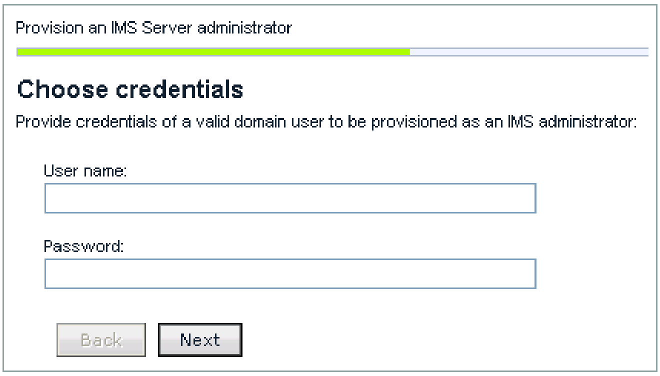
The configuration wizards simplify the IMS administrator provisioning workflow.

Provisioning IMS Administrators

To provision an IMS Administrator:

❶ Select *Configuration Wizards >> Provision IMS Administrator* from the IMS Configuration Utility navigation panel. The Choose credentials fields are displayed.

2. Enter the user name and password of a valid Active Directory user. This user will be provisioned on the IMS Server and automatically promoted to the Administrator role. Click **Next**.



Provision an IMS Server administrator

Choose credentials

Provide credentials of a valid domain user to be provisioned as an IMS administrator:

User name:

Password:

IMS Server Administrator credentials

3. The system displays a summary of the configured options. After reviewing the configuration settings, click **Finish.**

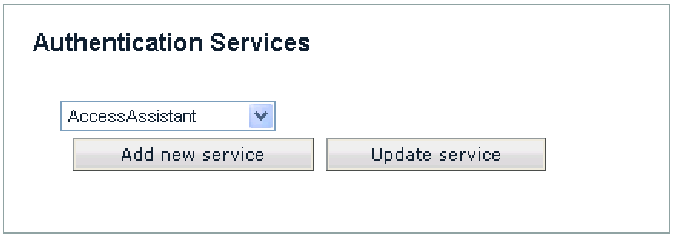
Modifying the IMS configuration keys (basic settings)

The IMS configuration keys are grouped according to complexity: basic or advanced.

Basic settings refer to the settings that govern the general behavior of the IMS Server, such as the types of authentication services and/or connectors used, the housekeeping schedule, support for biometrics, and all settings related to ActiveCode deployment.

Authentication services

To add a new authentication service, select *Basic Settings >> Authentication Services* from the IMS Configuration Utility navigation panel.



Authentication Services

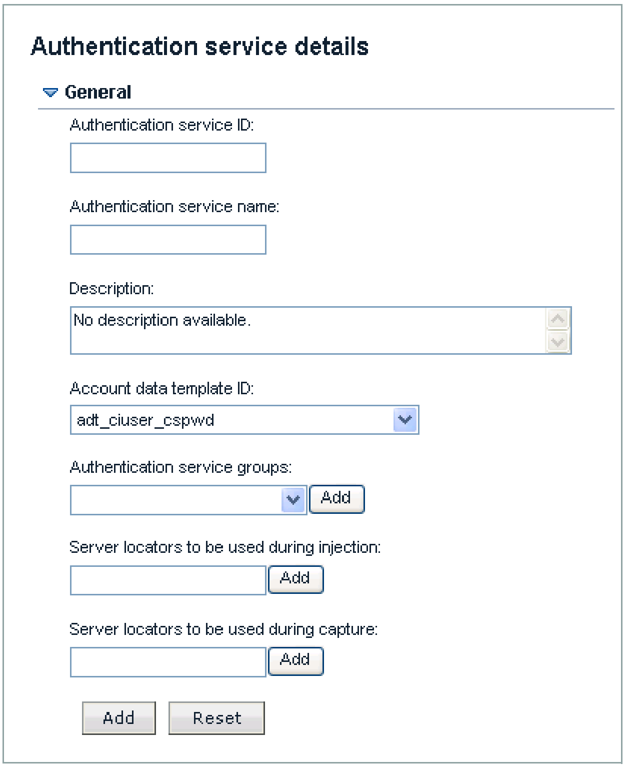
AccessAssistant

Authentication services

Click **Add new service** to set up a new service. To update an existing authentication service, select an authentication service from the drop-down list and click **Update service**.

Authentication services can also be created using the Encentuate AccessStudio. However, connectors for the authentication services can only be created using the IMS Configuration Utility.

Adding a new authentication service



Authentication service details

General

Authentication service ID:

Authentication service name:

Description: No description available.

Account data template ID: adt_ciuser_cspwd

Authentication service groups:

Server locators to be used during injection:

Server locators to be used during capture:

Authentication service details

- **Authentication service ID**

  Enter a unique identifier for the authentication service.

- **Authentication service name**

  Enter the name of the authentication service that will appear in the Wallet Manager.

- **Description**

  Enter a short description of the authentication service.

- Account data template ID

  Select an account data template ID from the drop-down list. The template ID defines the structure of the account data to be captured for the authentication service. For example, adt_ciuser_cspwd means the selected account data template will capture a case-insensitive user name and a case-sensitive password.

- Authentication service groups

  Select the authentication service’s group from the drop-down list and click **Add**.

- Server locators to be used during injection

  Enter the server locator’s name during auto-fill and click **Add**.

- Server locators to be used during capture

  Enter the server locator’s name during capture and click **Add**.

After specifying all the information, click **Add** to add the new authentication service.

Click **Reset** to discard changes.

Updating an authentication service

When you update a service, you can change any of the configuration keys in the form, except for the Authentication Service ID. For descriptions of the configuration keys, see Adding a new authentication service.

Click **Update** to confirm the changes.

Enterprise directories

An enterprise directory is a directory of user accounts that define IAM users. It validates user credentials during sign-up and logon, if Encentuate password is synchronized with the enterprise directory password. An example of an enterprise directory is an AD forest.

An enterprise directory may contain zero or more authentication services. An AD forest with multiple domains can be an enterprise directory that contains multiple authentication services, with each authentication service representing one domain.

A setup coupled with the password synchronization feature allows enterprise directory passwords to be used for both logon to Wallet and automatic sign-on to applications.

For simplicity purposes, an authentication service is always automatically created by the IMS Configuration Utility when an enterprise directory is created. The authentication service can be ignored if not used for application authentication.

About the enterprise directory connector

A connector should be defined for each enterprise directory, so that the IMS Server can communicate with it. The IMS Server uses the connector during sign-up or logon, to validate each user's credentials.

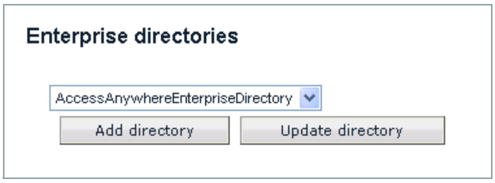
The connector is also used for searching the enterprise directory and obtaining user attributes such as email, phone number, etc. This same connector is automatically applied to all authentication services (AD domains) that belong to the enterprise directory, making it easier to create and maintain connectors for multiple AD domains.

With the enterprise directory defined, it becomes possible for IAM to identify a user by UPN (for example, "bob@encentuate.com", where "encentuate.com" may not be the same as the AD domain name.). This is because UPNs are unique across an AD forest, and the AD forest is represented in IAM by an enterprise directory.

As long as both the enterprise directory and UPN are known, IAM would be able to uniquely identify the user. This feature reduces the learning curve for users as it retains part of the look and feel, and behavior of the Windows logon prompt.

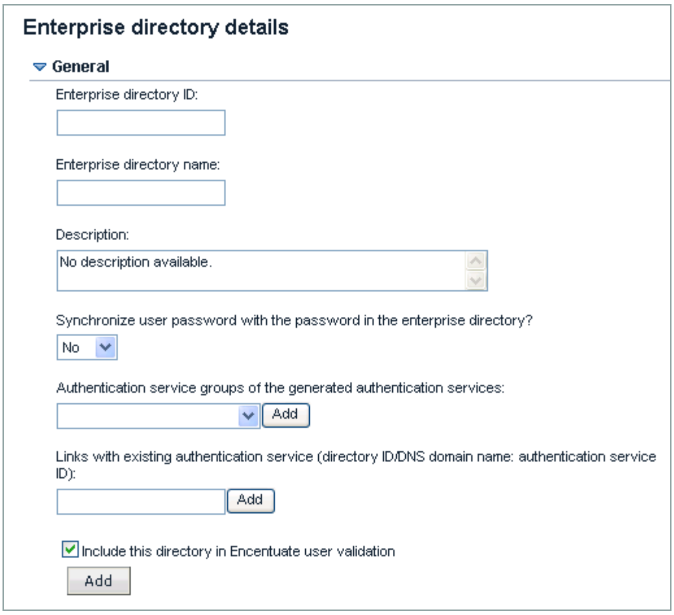
Adding new enterprise directories

To add a new directory, select *Basic Settings >> Enterprise directories* from the IMS Configuration Utility navigation panel. In Enterprise Directories, click Add directory.



Select a new directory

Modify the configuration keys in the form and click Add to create the new directory.



Enterprise directory details

General

Enterprise directory ID:

Enterprise directory name:

Description:

No description available.

Synchronize user password with the password in the enterprise directory?

No

Authentication service groups of the generated authentication services:

Links with existing authentication service (directory ID/DNS domain name: authentication service ID):

☑ Include this directory in Encentuate user validation

Enter the Enterprise directory details and click Add

- Enterprise directory ID

  The unique ID of the enterprise directory.

- Enterprise directory name

  The name of the enterprise directory to be displayed.

- Description

  This field contains a description of the enterprise directory, if desired by the Administrator.

- Synchronize user password with the password in the enterprise directory?

  Select Yes if Encentuate password is to be synchronized with the enterprise directory password. If enterprise directory is AD, this will be AD password synchronization.

  Select No if users are to use Encentuate passwords that are not synchronized with the enterprise directory passwords.

- Authentication service groups of the generated authentication services

  Select DomainAuthenticatorGroup. This is the authentication service group for Windows authentication. Click Add.

  This field can be modified only if you have created other authentication service groups for Windows authentication.

- Link with existing authentication service (directory ID/DNS domain name: authentication service ID)

  This field is important when upgrading the IMS Server. It maps the DNS domain name of each AD domain with existing authentication services.

  Specify the DNS domain names and authentication service IDs in the specified format (for example encentuate.com:dir_encentuate_domain). Click Add.

  Leave this field blank if you are performing a fresh IMS Server installation.

- Included in the enterprise directory list for Encentuate users validation?

  If this box is checked, this enterprise directory will be set as the enterprise directory for validating Encentuate users. Currently, only one enterprise directory is allowed in the list. If there is already an enterprise directory in the list, it will be replaced by the new enterprise directory.

Updating enterprise directories

To update an existing directory, select *Basic Settings >> Enterprise Directories* from the IMS Configuration Utility navigation panel. In Enterprise Directories, select a directory from the drop-down list and click Update directory.

Modify the configuration keys in the form and click Update to confirm the changes. For descriptions of the configuration keys, see Adding new enterprise directories.

Configuring Active Directory Service Interface (ADSI) connector

If the application uses Active Directory for authentication, configure the appropriate ADSI connector.

Basic Configuration Keys

- Application Connector

  The name of the connector.

- Specify the domain type to be shown in AccessAgent

  This field should be set to NetBIOS, so as to be consistent with the Windows logon interface.

Advanced Configuration Keys

- Record count limit

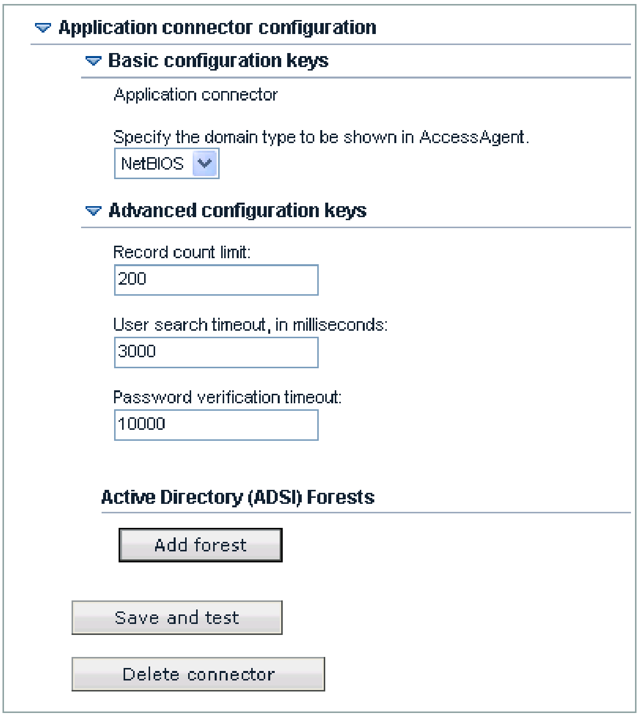
  The maximum number of user logons that are retrieved from the Active Directory Server when searching for users. Enter a number.

- User search timeout

  The time limit for searching and sending results. Exceeding this limit due to server load or network connection problems, etc. will result in a Timeout message to the user.

- Password verification timeout

  The time limit for verifying a password. If the server has not respond within the set value, the password verification attempt will be aborted.



Application connector configuration

Basic configuration keys

Application connector

Specify the domain type to be shown in AccessAgent.
NetBIOS

Advanced configuration keys

Record count limit:
200

User search timeout, in milliseconds:
3000

Password verification timeout:
10000

Active Directory (ADSI) Forests

Configure the application connector and click Save and Test

Active directory (ADSI) Forests

- Active Directory Server URI

  The hostname or IP address of the Active Directory Server. A non-default port number should be added after the hostname. For example: host123. Enter the hostname or IP address.

- Lookup user name (Provide in one of the following formats: domain\username e.g: corp\john OR UPN eg: john@corp.com)

  The Active Directory user name with permissions for lookup operations. If this is not set, the Active Directory server must be set to support anonymous connections. Enter the user name.

- Lookup user password

  The password for the user name with permissions for lookup operations. Enter the password.

- User tree DNs

  Distinguished Names (DNs) of the users in the Active Directory. Enter a name and click **Add**.

  Click **Remove** next to the corresponding DNs to delete.

Click **Add Forest** to create more forests.

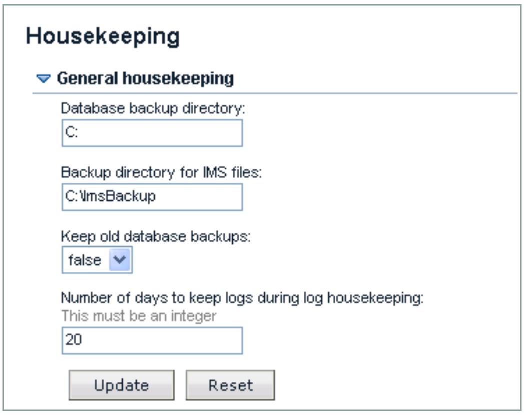
Click **Save and Test** to check if the connector has been configured correctly.

Click **Delete connector** to remove the connector.

IMS Server housekeeping

To perform IMS Server housekeeping tasks, select *Basic Settings >> IMS Server Housekeeping* from the IMS Configuration Utility navigation panel.

General housekeeping



Housekeeping

General housekeeping

Database backup directory: C:

Backup directory for IMS files: C:\ImsBackup

Keep old database backups: false

Number of days to keep logs during log housekeeping:
This must be an integer
20

Enter the housekeeping details and click Update

- Database backup directory

  Specifies the directory where RDB (Relational Database) backup files are to be stored. This directory must exist together with three subdirectories: daily, weekly and monthly. Any change to this parameter does **not** require restarting the Server.

This directory is created on the database server, **not** *the IMS Server. The daily, weekly and monthly subdirectories must also be created.*

Example of an accepted value: C:

- IMS Files backup directory

  Specifies the directory where Encentuate IMS backup files are to be stored. Any change to this parameter does not require restarting the Server.

  Example of an accepted value: C:\ImsBackup

- Keep old database backups?

  Using this parameter, you can specify if old RDB backup files should be kept in the Server. Any change to this parameter does not require restarting the Server.

  Possible values:

  - true - The last seven daily files, five weekly files, and 12 monthly files will be kept in the server.

  - false - No old backup files will be kept in the server.

  Select a value from the drop-down list.

- Number of days to keep logs during log housekeeping

  If you specify the value of this parameter as "X", logs from the last X days will be kept. Any change to this parameter does not require restarting the Server. Enter a number.

Click Update to save the new settings.

Click Reset to discard changes.

Daily housekeeping

- Enable daily housekeeping

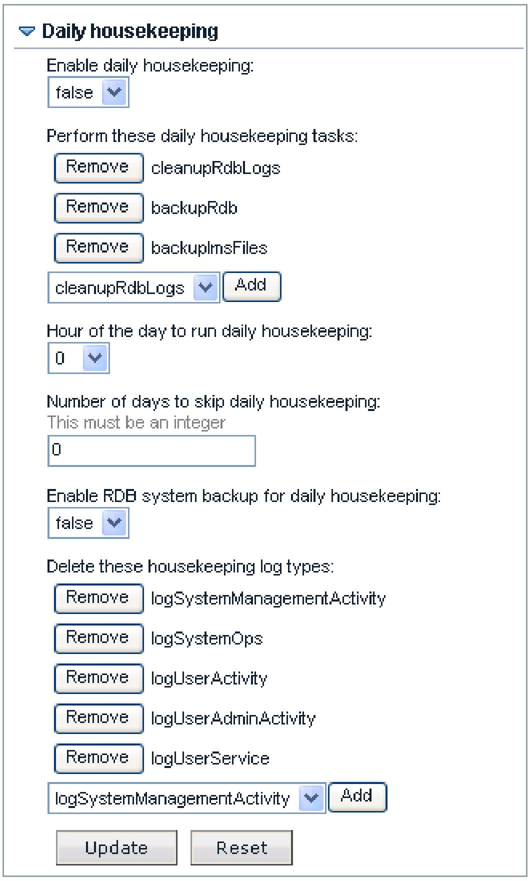
  This parameter specifies if daily housekeeping is enabled for the Encentuate IMS Server. Any change to the parameter value requires restarting the Server.

  Accepted values:

  - true - daily housekeeping is enabled

  - false - daily housekeeping is disabled.

  Select a value from the drop-down list.



Daily housekeeping

Enable daily housekeeping:
false

Perform these daily housekeeping tasks:
cleanupRdbLogs
backupRdb
backupImsFiles
cleanupRdbLogs

Hour of the day to run daily housekeeping:
0

Number of days to skip daily housekeeping:
This must be an integer
0

Enable RDB system backup for daily housekeeping:
false

Delete these housekeeping log types:
logSystemManagementActivity
logSystemOps
logUserActivity
logUserAdminActivity
logUserService
logSystemManagementActivity

Configure the housekeeping details and click Update

- Daily housekeeping tasks

The parameter specifies the daily housekeeping tasks that will be performed. Any change to the parameter value does **not** require restarting the Server.

The acceptable values vary, depending on the number and types of tasks you want to prescribe.

Currently, the following values are available:

- **cleanupRdbLogs** - activating this task causes database logs to be cleaned up every day
- **backupRdb** - this task creates a back up of the database every day
- **backupImsFiles** - this task creates a back up of the IMS files every day

Select a task from the drop-down list and then click **Add**.

To remove a task, click the **Remove** button next to the task.

- Daily housekeeping hour of the day

  Using this parameter, you can prescribe the daily start time of any housekeeping activity. Any change to this parameter requires restarting the Server.

  Accepted values: Any number between 0 and twenty-three (inclusive). Zero represents midnight.

  Enter a number.

- Daily housekeeping days to skip

  Specifies the number of days to skip until the next scheduled housekeeping is performed. Any change to the value of this parameter requires restarting the Server.

  Examples of acceptable values:

  - <1> means that housekeeping will be performed every other day.
  - <3> means housekeeping will be performed every three days.

  Enter a number.

- Daily housekeeping RDB system backup flag

  This parameter enables daily RDB (relational database) backup. In order to enable backup, the IMS user is required to have administrative privileges for the database. Any change to this parameter does not require restarting the Server.

  Possible values:

  - true - daily RDB backup is enabled.
  - false - daily RDB backup is disabled.

  Select a value from the drop-down list.

- Daily housekeeping log types to delete

  Using this parameter, you can specify the log types to be deleted daily. Any change to this parameter does not require restarting the Server. Select a log type from the drop-down list and then click Add.

  To remove a log type, click the Remove button next to the task.

Click Update to save the new settings.

Click Reset to discard changes.

Weekly housekeeping

- **Enable weekly housekeeping**

  This parameter specifies if weekly housekeeping is enabled for the Encentuate IMS Server. Any change to the parameter value requires restarting the Server.

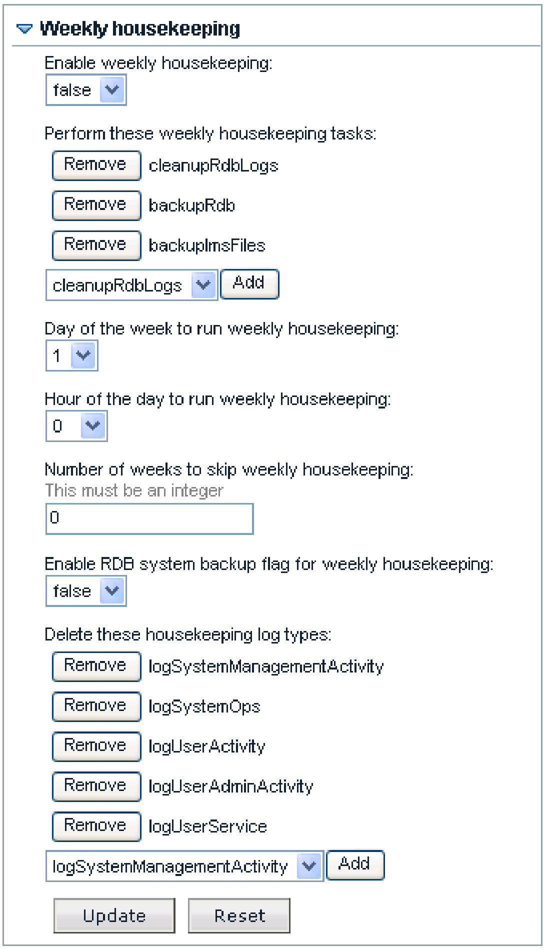
  Possible values:

  - true - weekly housekeeping is enabled.
  - false - weekly housekeeping is disabled.

  Select a value from the drop-down list.

- **Weekly housekeeping tasks**

  The parameter specifies the weekly housekeeping tasks that will be performed. Any change to the parameter value does not require restarting the Server.



Weekly housekeeping

Enable weekly housekeeping: false

Perform these weekly housekeeping tasks:

- cleanupRdbLogs
- backupRdb
- backupImsFiles

Day of the week to run weekly housekeeping: 1

Hour of the day to run weekly housekeeping: 0

Number of weeks to skip weekly housekeeping:
This must be an integer
0

Enable RDB system backup flag for weekly housekeeping: false

Delete these housekeeping log types:

- logSystemManagementActivity
- logSystemOps
- logUserActivity
- logUserAdminActivity
- logUserService

Configure the housekeeping details and click Update

The acceptable values vary, depending on the number and types of tasks you want to prescribe.

Currently, the following values are available:

- **cleanupRdbLogs** - activating this task causes database logs to be cleaned up every week
- **backupRdb** - this task creates a back up of the database every week
- **backupImsFiles** - this task creates a back up of the IMS files every week

Select a task from the drop-down list and then click **Add**.

To remove a task, click the **Remove** button next to the task.

- **Weekly housekeeping day of the week**

Using this parameter, you can prescribe the weekly start time of any housekeeping activity. Any change to this parameter requires restarting the Server.

Possible values:

- 1 - Sunday
- 2 - Monday
- 3 - Tuesday
- 4 - Wednesday
- 5 - Thursday
- 6 - Friday
- 7 - Saturday

Select a value from the drop-down list.

- **Weekly housekeeping start time in the day**

Using this parameter, you can prescribe the weekly start time of any housekeeping activity. Any change to this parameter requires restarting the Server.

Accepted values: Any number between 0 and twenty-three (inclusive). Zero represents midnight.

Select a value from the drop-down list.

- **Weekly housekeeping week(s) to skip**

  Specifies the number of week(s) to skip until the next scheduled housekeeping is performed. Any change to the value of this parameter requires restarting the Server.

  Examples of an acceptable value:

  - <1> means that housekeeping will be performed every other week.
  - <3> means housekeeping will be performed every three weeks.

  Enter a number.

- **Weekly housekeeping RDB system backup flag**

  This parameter enables weekly RDB (relational database) backup. In order to enable backup, the IMS User is required to have administrative privileges for the database. Any change to this parameter does not require restarting the Server.

  Possible values:

  - **true** - weekly RDB backup is enabled.
  - **false** - weekly RDB backup is disabled.

  Select a value from the drop-down list.

- **Weekly housekeeping log types to delete**

  Using this parameter, you can specify the log types to be deleted weekly. Any change to this parameter does not require restarting the Server. Select a log type from the drop-down list and then click **Add**.

  To remove a log type, click the **Remove** button next to the task.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Monthly housekeeping

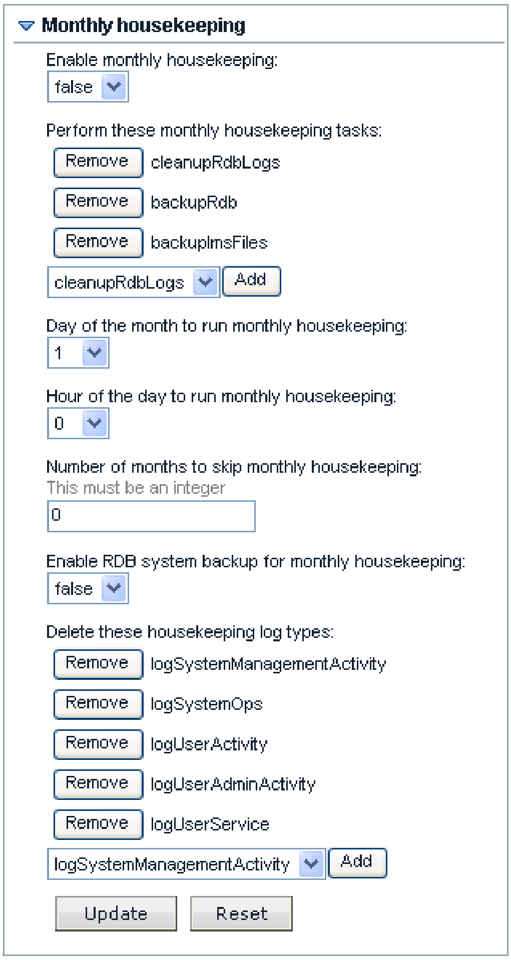
- **Enable monthly housekeeping**

  This parameter specifies if monthly housekeeping is enabled for the Encentuate IMS Server. Any change to the parameter value requires restarting the Server.

Possible values:

- **true** - monthly housekeeping is enabled.
- **false** - monthly housekeeping is disabled.

Select a value from the drop-down list.



Monthly housekeeping

Enable monthly housekeeping:
false

Perform these monthly housekeeping tasks:
cleanupRdbLogs
backupRdb
backupImsFiles
cleanupRdbLogs

Day of the month to run monthly housekeeping:
1

Hour of the day to run monthly housekeeping:
0

Number of months to skip monthly housekeeping:
This must be an integer
0

Enable RDB system backup for monthly housekeeping:
false

Delete these housekeeping log types:
logSystemManagementActivity
logSystemOps
logUserActivity
logUserAdminActivity
logUserService
logSystemManagementActivity

Configure the housekeeping details and click Update

Monthly housekeeping tasks

The parameter specifies the monthly housekeeping tasks that will be performed. Any change to the parameter value does not require restarting the Server.

The acceptable values vary, depending on the number and types of tasks you want to prescribe.

Currently, the following values are available:

- **cleanupRdbLogs** - activating this task causes database logs to be cleaned up every month

- **backupRdb** - this task creates a back up of the database every month

- **backupImsFiles** - this task creates a back up of the IMS files every month

Select a task from the drop-down list and then click **Add**.

To remove a task, click the **Remove** button next to the task.

- **Monthly housekeeping day**

  Using this parameter, you can prescribe the monthly start time of any housekeeping activity. Any change to this parameter requires restarting the Server.

  Possible values: Any number between 1 and thirty-one (inclusive).

  Select a value from the drop-down list.

- **Monthly housekeeping start time in the day**

  Using this parameter, you can prescribe the weekly start time of any housekeeping activity. Any change to this parameter requires restarting the Server.

  Accepted values: Any number between 0 and twenty-three (inclusive). Zero represents midnight.

  Select a value from the drop-down list.

- **Monthly housekeeping month(s) to skip**

  Specifies the number of month(s) to skip until the next scheduled housekeeping is performed. Any change to the value of this parameter requires restarting the Server.

  Examples of an acceptable value:

  - <1> means that housekeeping will be performed every other month.

  - <3> means housekeeping will be performed every three months.

  Enter a number.

- **Monthly housekeeping RDB system backup flag**

  This parameter enables monthly RDB (relational database) backup. In order to enable backup, the IMS User is required to have administrative privileges for the database. Any change to this parameter does not require restarting the Server.

Possible values:

- **true** - monthly RDB backup is enabled.
- **false** - monthly RDB backup is disabled.

Select a value from the drop-down list.

- **Monthly housekeeping log types to delete**

  Using this parameter, you can specify the log types to be deleted monthly. Any change to this parameter does not require restarting the Server.

  Select a log type from the drop-down list and then click **Add**.

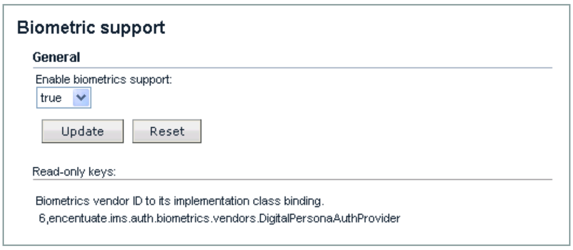
  To remove a log type, click the **Remove** button next to the task.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Biometric support

To enable or disable Biometrics support select *Basic Settings >> Biometric Support* from the IMS Configuration Utility navigation panel.



Biometric support

General

Enable biometrics support:
true

Read-only keys:

Biometrics vendor ID to its implementation class binding.
6,encentuate.ims.auth.biometrics.vendors.DigitalPersonaAuthProvider

Biometric support

- **Enable biometrics support**

  Using this configuration key, you can enable or disable biometrics support.

  Select a value from the drop-down list.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

ActiveCode deployment

To configure ActiveCode, select *Basic Settings >> ActiveCode Deployment* from the IMS Configuration Utility navigation panel.

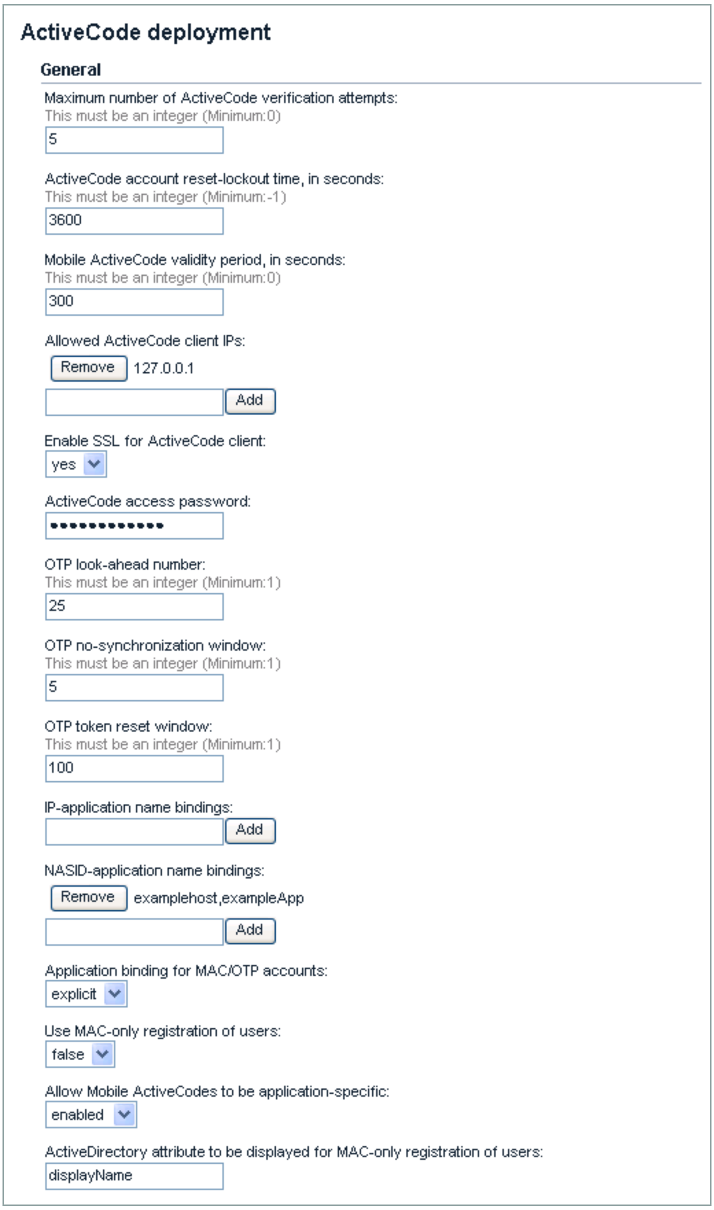
The following screenshot shows the first and second parts of the configuration keys.

- **Max ActiveCode verification attempts**

  You can use this configuration key to set the maximum number of incorrect Mobile ActiveCode entries allowed before the account gets locked. Enter a number.

- **ActiveCode account reset-lockout time in seconds**

  The waiting time before a locked Mobile ActiveCode gets reset (in milliseconds). Enter a number.



ActiveCode deployment

General

Maximum number of ActiveCode verification attempts:
This must be an integer (Minimum:0)
5

ActiveCode account reset-lockout time, in seconds:
This must be an integer (Minimum:-1)
3600

Mobile ActiveCode validity period, in seconds:
This must be an integer (Minimum:0)
300

Allowed ActiveCode client IPs:
127.0.0.1

Enable SSL for ActiveCode client:
yes

ActiveCode access password:
•••••••••••••

OTP look-ahead number:
This must be an integer (Minimum:1)
25

OTP no-synchronization window:
This must be an integer (Minimum:1)
5

OTP token reset window:
This must be an integer (Minimum:1)
100

IP-application name bindings:

NASID-application name bindings:
examplehost,exampleApp

Application binding for MAC/OTP accounts:
explicit

Use MAC-only registration of users:
false

Allow Mobile ActiveCodes to be application-specific:
enabled

ActiveDirectory attribute to be displayed for MAC-only registration of users:
displayName

ActiveCode Deployment: First Part

- Mobile ActiveCode validity period

  The length of time a Mobile ActiveCode is available for use. Enter a number.

- Allowed ActiveCode client IPs

  You must specify the IP address of the MAC-enabled application which will connect to the MAC Service Module of the IMS Server.

  Multiple VPN servers can point to the same IMS Server, and in such a case, enter all the IP addresses.

  Enter an IP address and then click Add.

  To remove an IP address, click the Remove button next to the corresponding IP address.

- SSL for ActiveCode client

  You must specify whether SSL access is required for the client making request/verify Mobile ActiveCode calls. Select Yes from the drop-down list to enable SSL. Select No from the drop-down list if you are using RADIUS.

- ActiveCode access password

  This is the shared secret between client and server for making Mobile ActiveCode calls. Enter the password.

- OTP look-ahead number

  The number of times an OTP should be generated in sequence from the seed for verification. Enter a number.

- OTP no-synchronization window

  The window size within which the OTP seeds will not be synchronized. Enter a number.

- OTP token reset window

  Number of OTPs to look ahead while resetting OTP tokens. Enter a number.

- IP-application name binding

  This is used for looking up the application name from the callers IP. Each entry is of the format IP:authentication service. Enter an IP-application name and then click Add.

  To remove an IP-application name, click the Remove button next to the corresponding IP-application name.

- NASID-application name binding

  This is used for looking up the application name from the callers NAS ID. Each entry is of the format IP:authentication service. Enter an NASID-application name and then click **Add**.

  To remove an NASID-application name, click the **Remove** button next to the corresponding NASID-application name.

- Application binding for MAC/OTP accounts

  This parameter sets the application binding properties.

  The possible values are:

  - Explicit: the logon ID need not be the same as enterprise ID. Users have to be explicitly allowed to use MAC.

  - Implicit: the logon ID is the enterprise ID.

  Select a value from the drop-down list.

- MAC-only registration of users

  This parameter specifies whether non-AccessAgent, MAC-only user-registration is supported. Select a value from the drop-down list.

- Allow Mobile ActiveCode to be application-specific

  Using this parameter, you can specify whether MACs are application-specific or are valid across applications. Select a value from the drop-down list.

- AD attribute to be displayed for MAC-only registration of users UI

  This is the AD attribute which is shown when users are searched on the User registration page. Enter an AD attribute.

- Should Mobile ActiveCodes be sent out in uppercase?

  This parameter determines whether MACs are sent out in uppercase or lowercase.

  Possible values:

  - true - MACs will be sent out in uppercase

  - false - MACs will be sent out in lowercase

- Search filter used for MAC-only registration of users UI

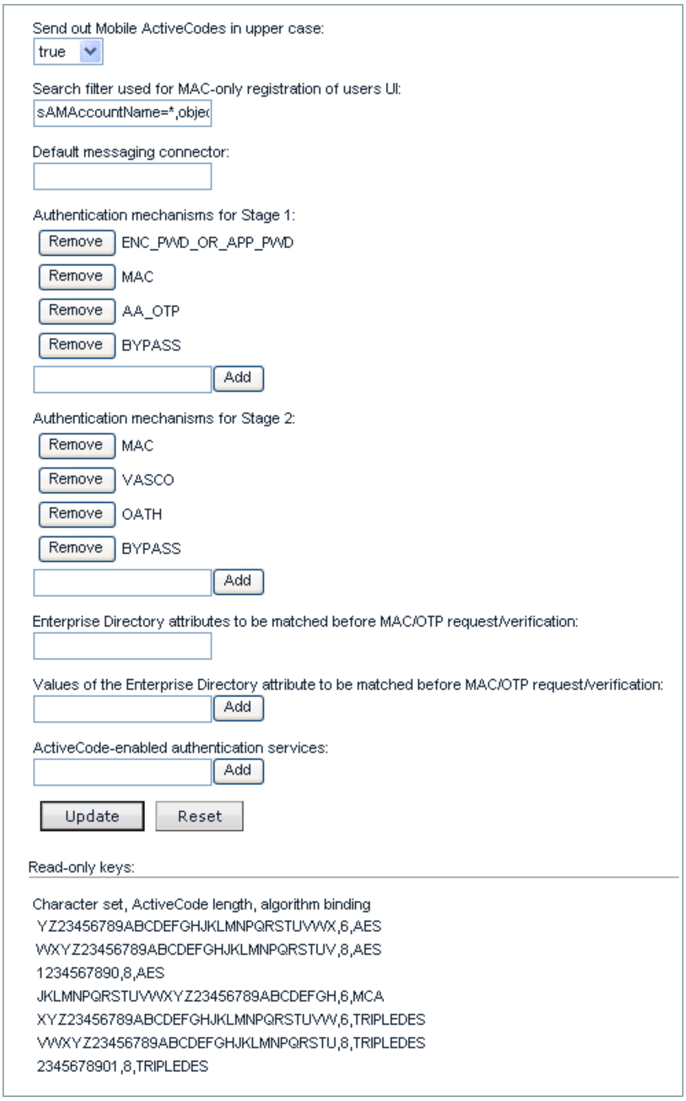
  This parameter specifies the comma-separated search filter used when users are searched on the User registration page.

Specify Name Value pairs in a comma-separated list such as the following:

For example: sAMAccountName=*,objectClass=user

- Default Messaging Connector

  Using this parameter, you can specify the default messaging connector. Enter the default messaging connector.



Send out Mobile ActiveCodes in upper case: true

Search filter used for MAC-only registration of users UI: sAMAccountName=*,objec

Default messaging connector:

Authentication mechanisms for Stage 1:

- ENC_PWD_OR_APP_PWD
- MAC
- AA_OTP
- BYPASS

Authentication mechanisms for Stage 2:

- MAC
- VASCO
- OATH
- BYPASS

Enterprise Directory attributes to be matched before MAC/OTP request/verification:

Values of the Enterprise Directory attribute to be matched before MAC/OTP request/verification:

ActiveCode-enabled authentication services:

Read-only keys:

Character set, ActiveCode length, algorithm binding
YZ23456789ABCDEFGHJKLMNPQRSTUVWX,6,AES
WXYZ23456789ABCDEFGHJKLMNPQRSTUV,8,AES
1234567890,8,AES
JKLMNPQRSTUVWXYZ23456789ABCDEFGH,6,MCA
XYZ23456789ABCDEFGHJKLMNPQRSTUVW,6,TRIPLEDES
VWXYZ23456789ABCDEFGHJKLMNPQRSTU,8,TRIPLEDES
2345678901,8,TRIPLEDES

ActiveCode Deployment: Second Part

- Authentication mechanisms for Stage 1

  This specifies the acceptable user inputs for stage 1 (authentication request) of a RADIUS Challenge-Response.

  It is an ordered list of one or more of the following values:

ENC_PWD_OR_APP_PWD: Encentuate password or application password.

MAC: Mobile ActiveCode.

AA_OTP: OTP generated by AccessAgent.

BYPASS: ActiveCode bypass (for example, authorization code + Encentuate password).

VASCO: OTP generated by VASCO time-based OTP token.

OATH: OTP generated by an OATH token.

- Authentication mechanisms for Stage 2

  This specifies the acceptable user inputs for stage 2 (response to challenge) of a RADIUS Challenge-Response. Note that if user is already authenticated using MAC or OTP in stage 1, the stage 2 authentication will be skipped.

  It is an ordered list of one or more of the following same values in Authentication mechanisms for Stage 1.

- Enterprise Directory attribute to be matched before MAC/OTP request/verification

  Specifies an Enterprise Directory attribute to be checked for before allowing MAC/OTP request/verification. This attribute should indicate whether the user is allowed to use MAC/OTP. If there is no such attribute, leave this setting empty.

  Limitations:

  • Only one attribute can be specified.

  • If set to true, performance will be degraded as each OTP/MAC request/verification makes a call to the Enterprise Directory.

  • To support fetching of multi-valued attributes (e.g memberOf), the ADSI connector should be used for configuring the Enterprise Directory.

- Values of the Enterprise Directory attribute to be matched before MAC/OTP request/verification

  This specifies a list of values for the Enterprise Directory attribute. If the user's Enterprise Directory attribute matches any of the values in this list, the user is allowed to use MAC/OTP.

  Both single and multi-valued attributes are supported. For multi-valued attributes (for example memberOf), user is allowed to use MAC/OTP as long as one of the values matches any of the values in the list. For the memberOf attribute, the values are the Distinguished Names (DN), for example cn=Domain Users, dc=encentuate, and dc=com".

Click **Update** to save the new settings.

Click **Reset** to discard changes.

- Character set, ActiveCode length, algorithm binding

  These parameters are set during deployment and cannot be modified. You can only view the parameters using the IMS Configuration Utility.

  ```
  YZ23456789ABCDEFGHJKLMNPQRSTUVWX,6,AES

  WXYZ23456789ABCDEFGHJKLMNPQRSTUV,8,AES

  1234567890,8,AES

  JKLMNPQRSTUVWXYZ23456789ABCDEFGH,6,MCA

  XYZ23456789ABCDEFGHJKLMNPQRSTUVW,6,TRIPLEDES

  VWXYZ23456789ABCDEFGHJKLMNPQRSTU,8,TRIPLEDES
  ```

  The parameter used for MAC is JKLMNPQRSTUVWXYZ23456789ABCDEFGH,6,MCA

Modifying the IMS configuration keys (advanced settings)

In the advanced settings section, you can modify configuration keys relating to the more advanced level of behavior of Encentuate IAM.

AccessAdmin

To configure AccessAdmin, select *Advanced Settings >> AccessAdmin* from the IMS Configuration Utility navigation panel.

User interface

Shown are the first, second, and third parts of the User Interface configuration keys.

- IMS server name

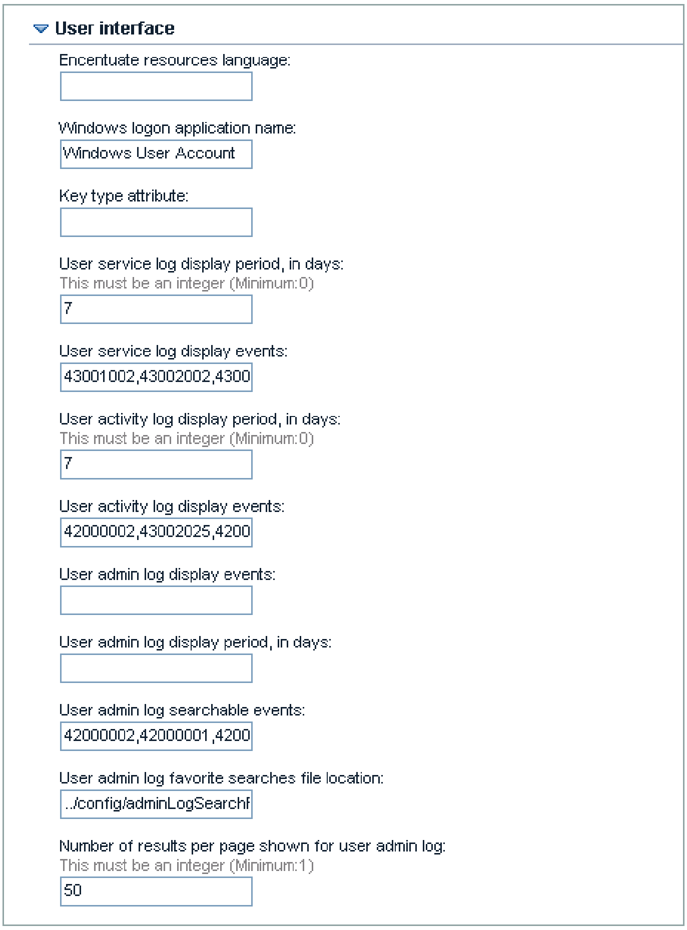
  This is the name of the IMS Server. Enter a name.

- Encentuate resources language

  Here, you must specify a valid ISO Language Code. These codes are the lower-case, two-letter codes as defined by ISO-639. Enter a language code.

- **Windows logon application name**

  This is the name of the application that Windows logon accounts will be displayed as being accounts of. Enter a name.



User interface

Encentuate resources language:

Windows logon application name:
Windows User Account

Key type attribute:

User service log display period, in days:
This must be an integer (Minimum:0)
7

User service log display events:
43001002,43002002,4300

User activity log display period, in days:
This must be an integer (Minimum:0)
7

User activity log display events:
42000002,43002025,4200

User admin log display events:

User admin log display period, in days:

User admin log searchable events:
42000002,42000001,4200

User admin log favorite searches file location:
../config/adminLogSearchf

Number of results per page shown for user admin log:
This must be an integer (Minimum:1)
50

AccessAdmin >> User Interface: First Part

- **Key type attribute**

  Specifies the attribute that provides information about the type of key being used. The entry here must match a SID attribute in IMSAttribut-Name table in the database. For example, the value tokenType. Enter an attribute.

- **User service log display period**

  Specifies the number of days, user service logs are displayed. The default value is 10 days. Enter a number.

- **User service log display events**

  Specifies which user service events to display in the Encentuate IMS Server user interface. The event codes are in hexadecimal and correspond to the codes declared in encentuate.ims.common.EventCode. Enter an event.

- User activity log display period

  Specifies the number of days, user logs will be displayed. The default value is 10 days. Enter a number.

- User activity log display events

  Specifies which user events to display in the Encentuate IMS Server user interface. The event codes are in hexadecimal and correspond to the codes declared in encentuate.ims.common.EventCode. Enter an event.

- User admin log display events

  Specifies which Helpdesk events to display in the Encentuate IMS Server user interface. The event codes are in hexadecimal and correspond to the codes declared in encentuate.ims.common.EventCode. Enter an event.

- User admin log display period

  Specifies the number of days, Helpdesk logs are displayed. The default is 10 days. Enter a number.

- User admin log searchable events

  Specifies which events should be searchable on IMS UI. The value is a comma-separated list of the event codes in Hex. Enter an event.

- User admin log favorite searches file

  Specifies where the file containing the User Admin Log favorite searches should be stored. Enter a location where the file is to be stored.

- User admin log results-per-page

  The number of log entries to show per page for the User Admin Log Page. Enter a number.

- System logs kept in memory

  The amount (in KB) of system logs to keep in memory. These logs are displayed on the 'status' page of AccessAdmin. Enter a number.

- Policy assignment attribute

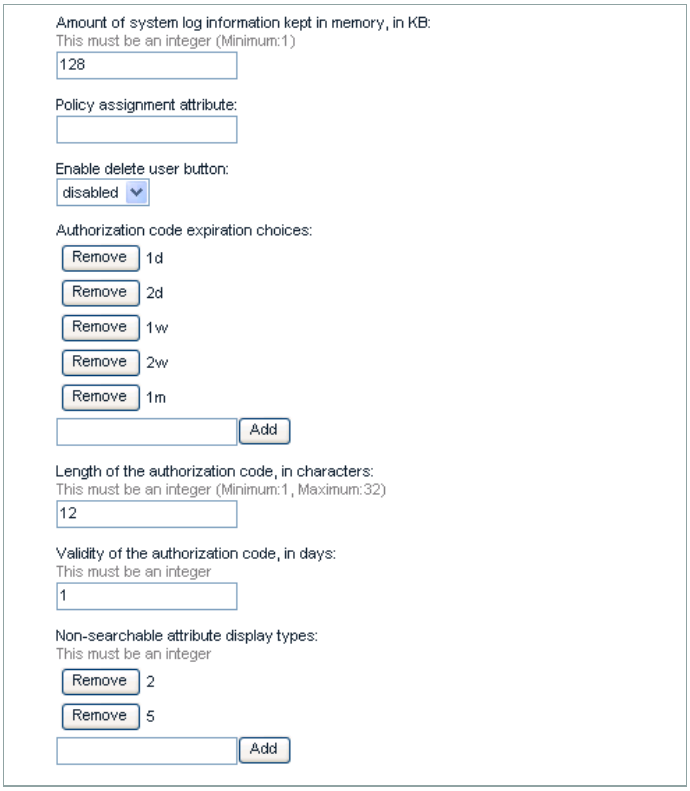
  This is the attribute based on whose value the policy templates are applied to users during registration. Enter an attribute.

- Delete user button

  This parameter specifies whether the delete user option is available on AccessAdmin.

- **true** - the **delete user** button is available
- **false** - the **delete user** button is disabled.

Select a value from the drop-down list.



Amount of system log information kept in memory, in KB:
This must be an integer (Minimum:1)
128

Policy assignment attribute:

Enable delete user button:
disabled

Authorization code expiration choices:
Remove 1d
Remove 2d
Remove 1w
Remove 2w
Remove 1m
Add

Length of the authorization code, in characters:
This must be an integer (Minimum:1, Maximum:32)
12

Validity of the authorization code, in days:
This must be an integer
1

Non-searchable attribute display types:
This must be an integer
Remove 2
Remove 5
Add

AccessAdmin > User Interface: Second Part

Authorization code expiry choices

Shows the different expiry times possible for authorization code expiry on AccessAdmin. Each value is made from a number and a letter. The letter can be from the set {h, d, w, m} corresponding to {hour, day, week, month} respectively. The number represents how many hours/days/weeks/months (For example: 1d is 1 day, 2w is 2 weeks). Enter an expiry time and then click **Add**.

To remove an expiry time, click the **Remove** button next to the expiry time.

Length of the authorization code

The length of the authorization code. Enter a number between 1 and 32 (inclusive).

Validity of the authorization code in days

This parameter specifies how long the authorization code is valid for. The validity period is specified in number of days. Enter a number.

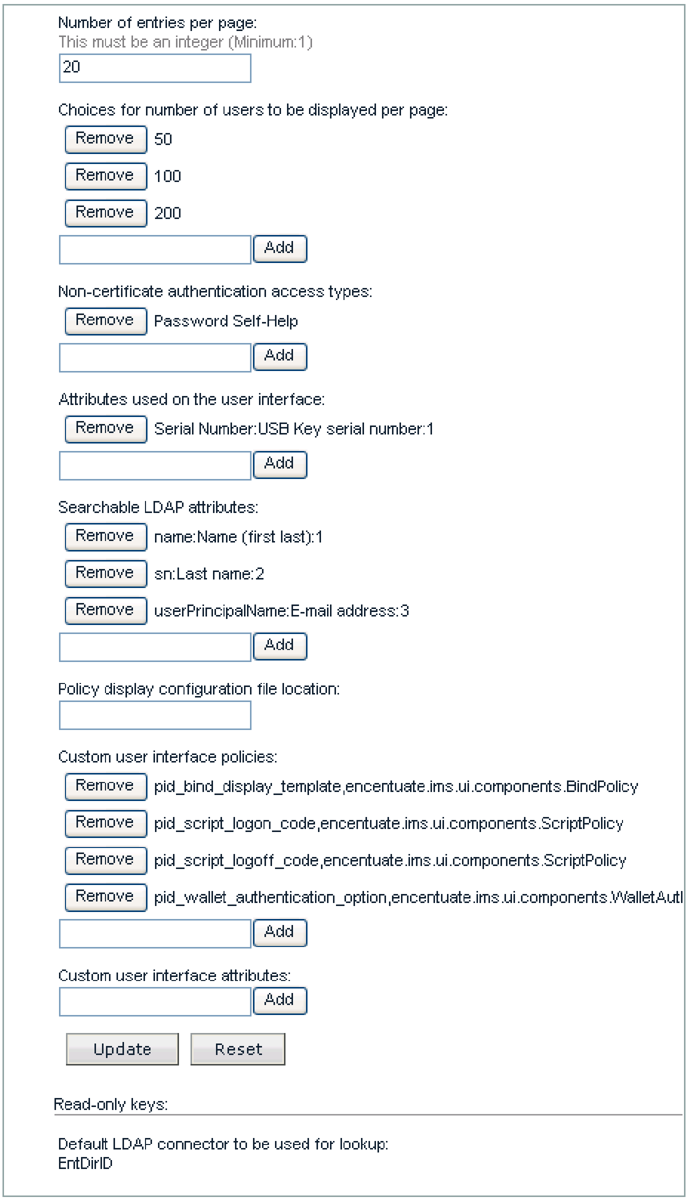
- Non-searchable attribute display types

  These are the attribute display types which are not searchable on AccessAdmin. Enter a display type and then click **Add**.

  To remove a display type, click the **Remove** button next to the display type.

- Entries per page

  The number of entries to be displayed on a page on AccessAdmin. Enter a number.



Number of entries per page:
This must be an integer (Minimum:1)
20

Choices for number of users to be displayed per page:
50
100
200

Non-certificate authentication access types:
Password Self-Help

Attributes used on the user interface:
Serial Number:USB Key serial number:1

Searchable LDAP attributes:
name:Name (first last):1
sn:Last name:2
userPrincipalName:E-mail address:3

Policy display configuration file location:

Custom user interface policies:
pid_bind_display_template,encentuate.ims.ui.components.BindPolicy
pid_script_logon_code,encentuate.ims.ui.components.ScriptPolicy
pid_script_logoff_code,encentuate.ims.ui.components.ScriptPolicy
pid_wallet_authentication_option,encentuate.ims.ui.components.WalletAutl

Custom user interface attributes:

Read-only keys:

Default LDAP connector to be used for lookup:
EntDirID

AccessAdmin > User Interface: Third Part

- Non-certificate authentication access types

  The access types for non-certificate authentication. Enter an access type and then click Add.

  To remove an access type, click the Remove button next to the access type.

- Attributes used on the UI

  These are the attributes that AccessAdmin uses along with their display names, and display types. Enter an attribute and then click Add.

  To remove an attribute, click the Remove button next to the attribute.

- Searchable LDAP attributes

  These declare all the LDAP attributes that IMS supports querying on. The format is [LDAP Attribute]:[Display Name]:[Display Order]. Enter an attribute and then click Add.

  To remove an attribute, click the Remove button next to the attribute.

- Policy display configuration file

  The file that determines the policies and what order to display them on the AccessAdmin UI. Enter a file name.

- Custom user interface policies

  Policies that have custom user interfaces. The value should be in the format of a comma-separated policy ID and class name. For example: pid_bind, encentuate.ims.ui.component.Binder. Enter a policy and then click Add.

  To remove a policy, click the Remove button next to the policy.

- Custom user interface attributes

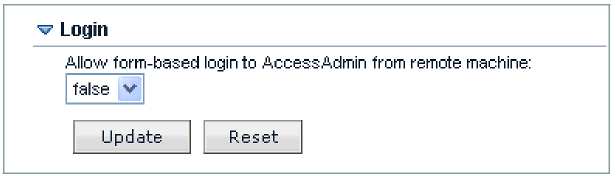
  Attributes that have custom user interfaces. The value should be in the format of a comma-separated attribute name and class name (eg.gsmNumber, encentuate.ims.ui.component.GsmNumber). Enter an attribute and then click Add.

  To remove an attribute, click the Remove button next to the attribute.

Click Update to save the new settings.

Click Reset to discard changes.

Login



Login

Allow form-based login to AccessAdmin from remote machine: false

- **Allow form-based login to AccessAdmin from remote machine**

  Specifies form-based login should be allowed for AccessAdmin from outside the machine where IMS is installed. If set to **false**, only SCR login is allowed. The default setting is **false**.

  Click **Update**.

Session

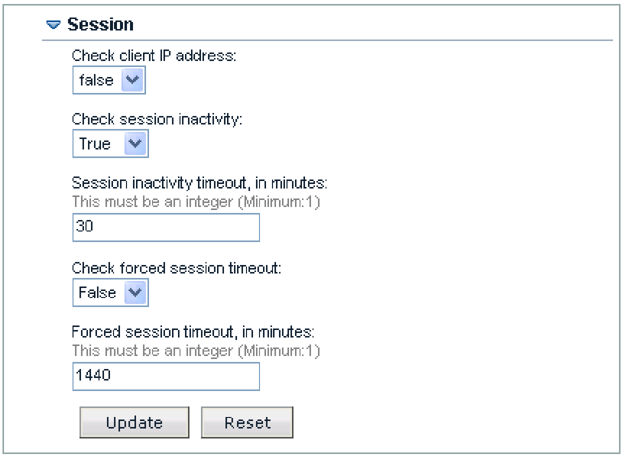
- **Check client IP address**

  This parameter specifies if the client's IP address should be checked during session validation. This restricts a session to the IP address it was created from.

  The default value is **false**.

  - **true** - the client's IP address will be checked.
  - **false** - the client's IP address will not be checked.

  Select a value from the drop-down list.



Session

Check client IP address: false

Check session inactivity: True

Session inactivity timeout, in minutes:
This must be an integer (Minimum:1)
30

Check forced session timeout: False

Forced session timeout, in minutes:
This must be an integer (Minimum:1)
1440

- Check session inactivity

  This parameter specifies if sessions should be timed out because of inactivity. Defaults to true if not specified.

  - true - session times out after a period of inactivity.
  - false - session does not time out.

  Select a value from the drop-down list.

- Session inactivity timeout in minutes

  The Inactivity timeout in minutes. The default value is 15 minutes. Enter a number.

- Check forced session timeout

  Specifies if the client should be forced to re-logon after a fixed period of time. Defaults to false if not specified.

  - true - client will be forced to logon after a period of inactivity
  - false - session does not time out.

  Select a value from the drop-down list.

- Forced session timeout in minutes

  The forced timeout in minutes. Defaults to one day (1440 minutes). Enter a number.

User attributes

- Initial IMS Admin Encentuate user names

  The enterprise IDs which will automatically be promoted to the Administrator role when they are registered. Enter an enterprise ID and then click Add.

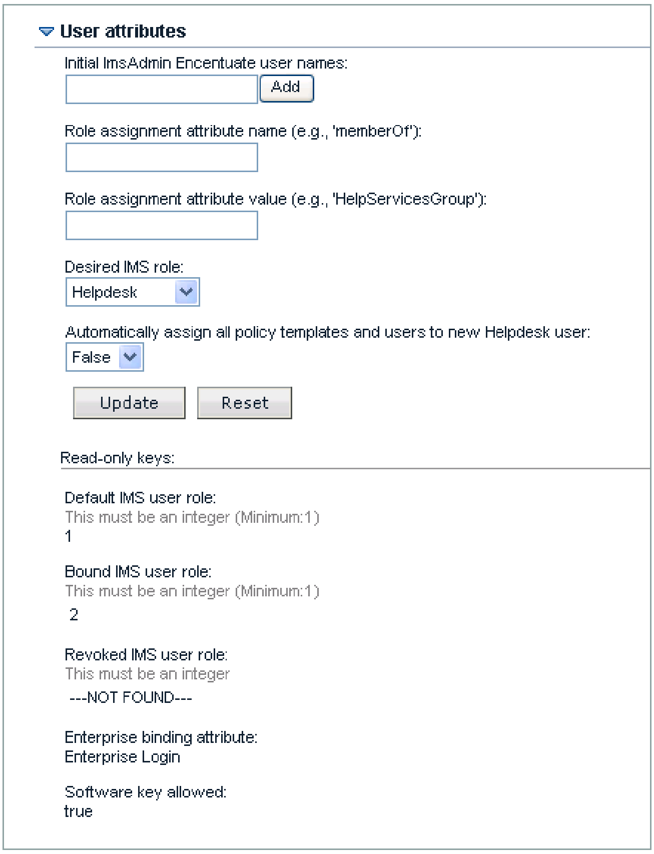
  To remove an enterprise ID, click the Remove button next to the enterprise ID.

- Role assignment attribute name, for example memberOf

  The name of an AD attribute used as a criterion for IMS role assignment.

- Role assignment attribute value, for example HelpServicesGroup

  The key of role assignment mapping (an AD attribute value). Multiple values should be separated by a semicolon (;).



User attributes

Initial ImsAdmin Encentuate user names:

Role assignment attribute name (e.g., 'memberOf'):

Role assignment attribute value (e.g., 'HelpServicesGroup'):

Desired IMS role:
Helpdesk

Automatically assign all policy templates and users to new Helpdesk user:
False

Read-only keys:

Default IMS user role:
This must be an integer (Minimum:1)
1

Bound IMS user role:
This must be an integer (Minimum:1)
2

Revoked IMS user role:
This must be an integer
---NOT FOUND---

Enterprise binding attribute:
Enterprise Login

Software key allowed:
true

User attributes

- Desired IMS role

  The value of role assignment mapping (a valid IMS role).

- Default assignment of all policy templates and users to new HelpDesk user

  Automatically assign all existing users and policy templates to any newly created Helpdesk user.

The following parameters are set during deployment and cannot be modified. You can only view the parameters using the IMS Configuration Utility.

- Default IMS user role

  Upon registration, the user’s role is set to 1 (unbound user). There must be a matching entry in the IMSRole table of the database under roleID.

- Bound IMS user role

  Once registration of the user is successful, the user’s role is set to 2 (user). Multiple entries can be specified for multiple roles. There must be a matching entry in the IMSRole table of the database under roleID.

- Revoked IMS user role

  The role that user will have after revocation.

- Enterprise binding attribute

  Enterprise bind attribute to create on successful binding. This must match one of the attrName fields in IMSAttributeName table.

- Software key allowed

  This parameter determines whether software keys are allowed. Click **Update** to save the new settings.

  Click **Reset** to discard changes.

Feedback email

- SMTP server URI

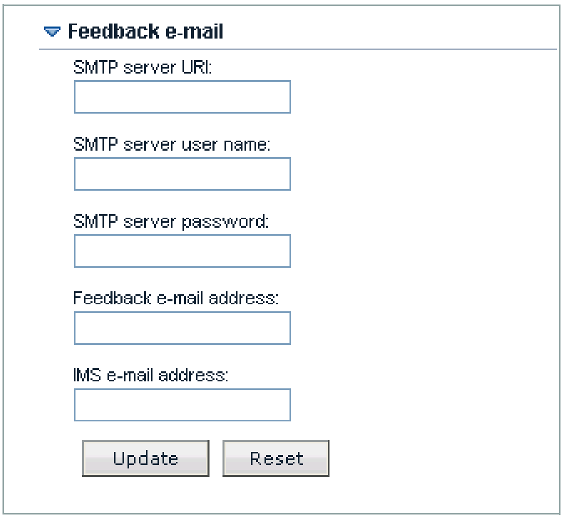
  The URI of the SMTP server which will be used to send e-mails. Enter the URI.

- SMTP server user name

  The user name to authenticate to the SMTP Server. This must be a valid user name on the SMTP mail server. Enter the user name.

- SMTP server password

  The corresponding password for the user name used to authenticate to the mail server. Enter the password.



Feedback e-mail

- Feedback email address

  The email address to which feedback submitted by users will be sent. Enter an email address.

- IMS email address

  The email address that will appear in the from field for e-mails sent from the IMS Server. Enter an email address.

  Click **Update** to save the new settings.

  Click **Reset** to discard changes.

IMS Server

To configure IMS Server, select *Advanced Settings >> IMS Server* from the IMS Configuration Utility navigation panel.

Logging

Logging-to-file

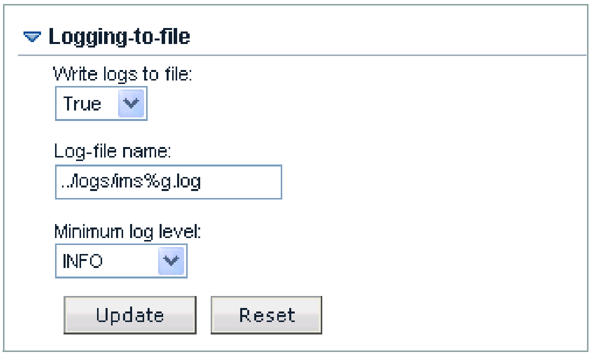
Using this configuration key, you can specify the location of the audit logs in the directory.

- Write logs to file

  This parameter specifies whether the IMS logs are logged to a file that can be viewed using log factor 5.

  - true - IMS log file can be viewed using log factor 5.
  - false - IMS log file cannot be viewed using log factor 5.

  Select a value from the drop-down list.



Logging-to-file

Write logs to file: True

Log-file name: ../logs/ims%g.log

Minimum log level: INFO

Logging-to-file

- Log-file name

  Specifies the name and the location of the IMS log files. For example: ../logs/ims%g.log where the %g will be replaced by a number to create a set of log files. Enter the name and location of the IMS log files.

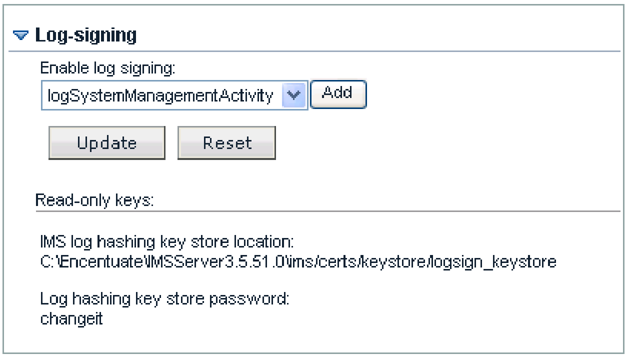
- Minimum log level

  Specifies the minimum log level that will be logged to file. In increasing order, the levels are: FINEST, FINER, FINE, CONFIG, INFO, WARNING, SEVERE. Select a log level from the drop-down list.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Log-signing



Enable log signing:
logSystemManagementActivity

Read-only keys:

IMS log hashing key store location:
C:\Encentuate\IMSServer3.5.51.0\ims/certs/keystore/logsign_keystore

Log hashing key store password:
changeit

Log-signing

- Log signing enabled

  This is the list of tables for which the logs will be hashed and signed. The available tables are: logSystemManagementActivity, logSystemOps, logUserAdminActivity, logUserService, logUserActivity. Select a table from the drop-down list and then click **Add**.

  To remove a table from the list, click the **Remove** button next to the table name.

  The following parameters are set during deployment and cannot be modified. You can only view the parameters using the IMS Configuration Utility.

  - IMS log hashing keystore store location

    This is the keystore that contains the private key for log hashing in IMS.

  - Log hashing keystore password

    The password for Keystore that contains the private key for log hashing.

Click **Update** to save the new settings.

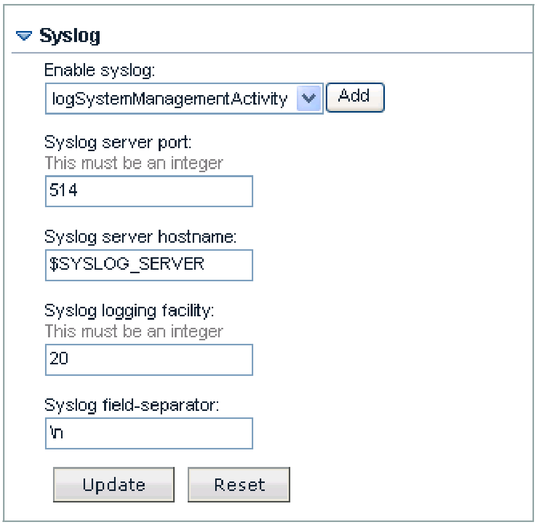
Click **Reset** to discard changes.

Syslog

- **Syslog enabled**

  This is the list of tables for which the logs will logged to the syslog server. The available tables are: logSystemManagementActivity, logSystemOps, logUserAdminActivity, logUserService, logUserActivity. Select a table from the drop-down list and then click **Add**.

  To remove a table from the list, click the **Remove** button next to the table name.



Syslog

Enable syslog: logSystemManagementActivity

Syslog server port: This must be an integer 514

Syslog server hostname: $SYSLOG_SERVER

Syslog logging facility: This must be an integer 20

Syslog field-separator: \n

Syslog

- **Syslog server port**

  The port number at which the syslog daemon is listening. Enter a port number.

- **Syslog server hostname**

  The hostname of the syslog server. Enter the hostname.

- **Syslog logging facility**

  The integer value of the facility used for logging to the syslog server. Enter a number.

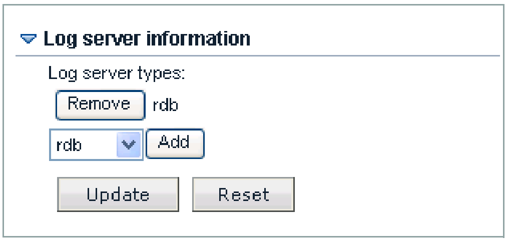
- **Syslog field-separator**

  Separator character used for separating name/value pairs in a log entry. For example: “\n” (Line feed). Enter the field separator.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Log server information



Log server information

Log server types:

Remove rdb

rdb Add

Log server information

- Log server type

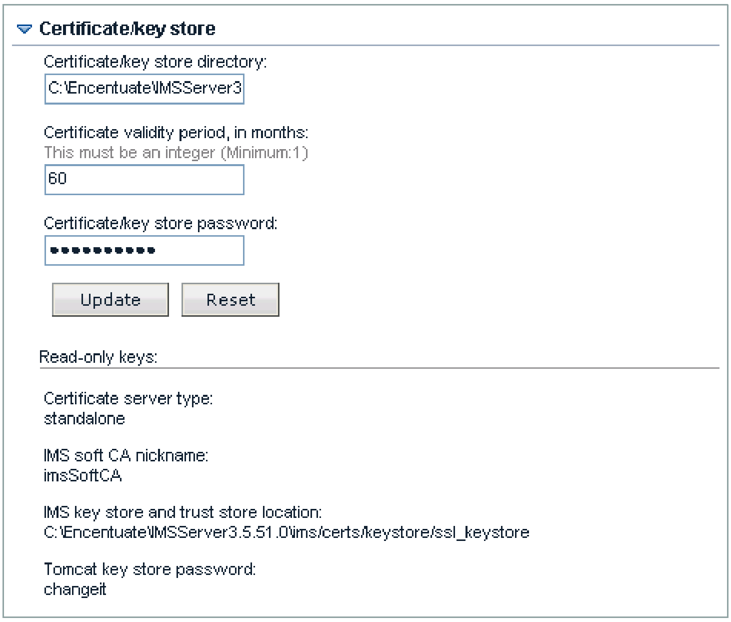
  Type(s) of log server(s) used as IMS log data store.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Certificate

Certificate/Keystore



Certificate/key store

Certificate/key store directory:
C:\Encentuate\IMSServer3

Certificate validity period, in months:
This must be an integer (Minimum:1)
60

Certificate/key store password:
●●●●●●●●●●●

Read-only keys:

Certificate server type:
standalone

IMS soft CA nickname:
imsSoftCA

IMS key store and trust store location:
C:\Encentuate\IMSServer3.5.51.0\ims/certs/keystore/ssl_keystore

Tomcat key store password:
changeit

Certificate/keystore

- Certificate/keystore directory

  The location of the certificate/keystore. Enter a location.

- Certificate validity period in months

  This is the number of months that certificates issued will be valid for. Enter a number.

- Certificate/keystore password

  The password for network security services keystore. When run for the first time, it is encrypted and appears in the ciphertext section. Enter the password.

The following parameters are set during deployment and cannot be modified. You can only view the parameters using the IMS Configuration Utility.

- Certificate server type

  This parameter specifies if this server contains a standalone certificate server as opposed to a proxy. However, currently only a standalone certificate server implementation is supported.

- IMS soft CA nickname

  The alias for the certificate authority (CA) certificate in the certificate store.

- IMS keystore and trust store location

  The location of the keystore and trust store for IMS.

- Tomcat keystore password

  Password for IMS key and trust store.

Click Update to save the new settings.

Click Reset to discard changes.

CRL Publication

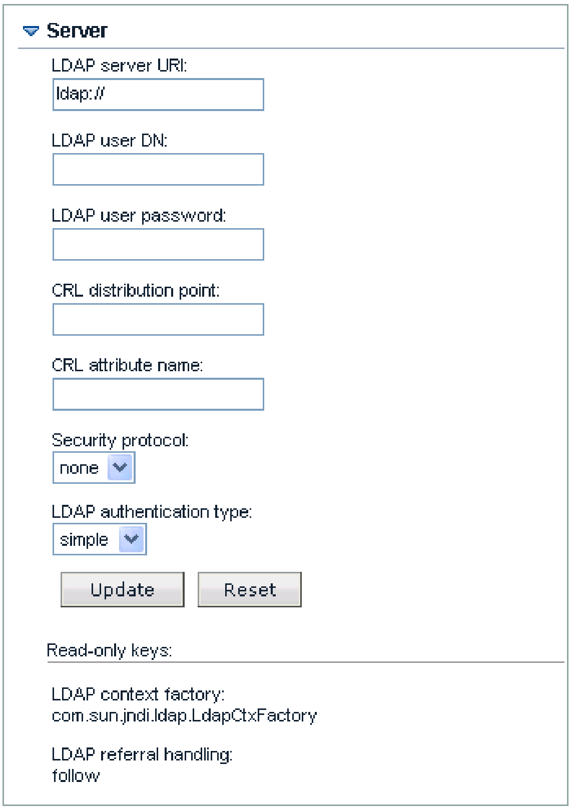
Server

- LDAP server URI

  URI of the LDAP server to which IMS server publishes CRL. For example, “ldap://machinename”.

- **LDAP user DN**

  The Distinguished Name (DN) of a lookup user in the LDAP server. If the remote LDAP server is an ActiveDirectory (AD), this value can also be the sAMAccountName of the lookup user.



Server

LDAP server URI:
ldap://

LDAP user DN:

LDAP user password:

CRL distribution point:

CRL attribute name:

Security protocol:
none

LDAP authentication type:
simple

Read-only keys:

LDAP context factory:
com.sun.jndi.ldap.LdapCtxFactory

LDAP referral handling:
follow

Server

- **LDAP user password**

  Password of the LDAP lookup user.

- **CRL distribution point**

  Distinguished Name (DN) of a node to which IMS publish CRL in the remote LDAP server.

- **CRL attribute name**

  Name of the ldap attribute of the **crlDistributionPoint** node that contains CRL. In most of the Ldap servers, the value should be **certificateRevocationList;binary**.

- LDAP context factory

  Fully qualified class name of the factory class that will create an initial context. This configuration is optional. Default value is com.sun.jndi.ldap.LdapCtxFactory.

- Security protocol

  Security protocol used for communication between IMS and the LDAP server. Valid values are ssl and none. ssl means IMS talks with LDAP server with SSL protocol; none means no security protocol is used. This configuration is optional, default value is none.</description>

- LDAP authentication type

  Type of authentication that IMS need to perform to login to the LDAP server. Valid values are none, simple, strong. none means no authentication. simple means password based authentication. strong means certificate based authentication. This configuration is optional, default value is simple.

- LDAP referral handling

  This key specifies how referrals returned by the LDAP server are to be processed. Valid values include follow and ignore. follow means IMS follows referrals automatically. ignore means IMS ignores referrals. This configuration is optional, default value is follow.

Click Update to save the new settings.

Click Reset to discard changes.

Re-publication on failures

- LDAP referral handling enabled

  A switch to enable/disable CRL re-publication when one CRL publication fails.

- Maximum re-publication attempts

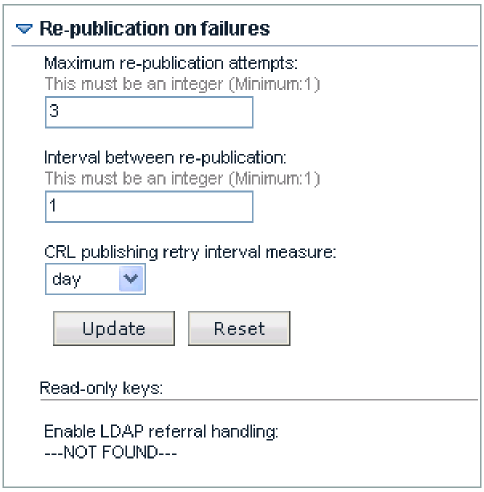
  Maximum number of retries when a CRL publication fails. It can be any positive integer and default value is 3.

- Interval between re-publication

  Length of interval between two CRL publication retries. It can be any positive integer, default value is 1.

- CRL publishing retry interval measure

  Measure of the length of retry interval. It can be either day, hour, minute, or second. Default value is minute.



Re-publication on failures

Maximum re-publication attempts:
This must be an integer (Minimum:1)
3

Interval between re-publication:
This must be an integer (Minimum:1)
1

CRL publishing retry interval measure:
day

Read-only keys:

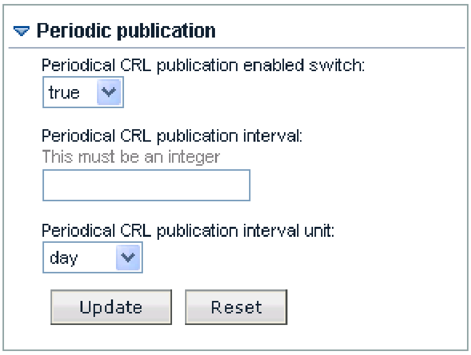
Enable LDAP referral handling:
---NOT FOUND---

Re-publication on failures

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Periodic publication



Periodic publication

Periodical CRL publication enabled switch:
true

Periodical CRL publication interval:
This must be an integer

Periodical CRL publication interval unit:
day

Periodic publication

- Periodical CRL publication enabled switch

  A switch to enable/disable periodical CRL publication.

- Periodical CRL publication interval

  Length of time interval between two periodic publications. It can be any positive integer. If this key is not configured or if it is set to -1, periodic CRL publication is disabled.

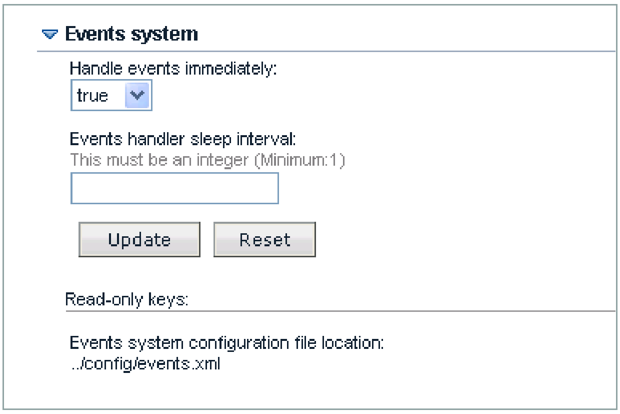
- Periodical CRL publication interval measure

  Measure of length of periodic CRL publication interval. It can be either **day**, **hour**, **minute**, or **second**.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Events system



Events system

Handle events immediately:
true

Events handler sleep interval:
This must be an integer (Minimum:1)

Read-only keys:

Events system configuration file location:
../config/events.xml

Events system

- **Handle events immediately**

  Specifies if the event system should handle events immediately. If this is set to true then the sleep interval is ignored.

- **Events handler sleep interval**

  Specifies how often the Event Controller should check for events. Used only if encentuate.events.HandleImmediately is set to false.

  Click **Update** to save the new settings.

  Click **Reset** to discard changes.

JMX

- **JMX HTTP port number**

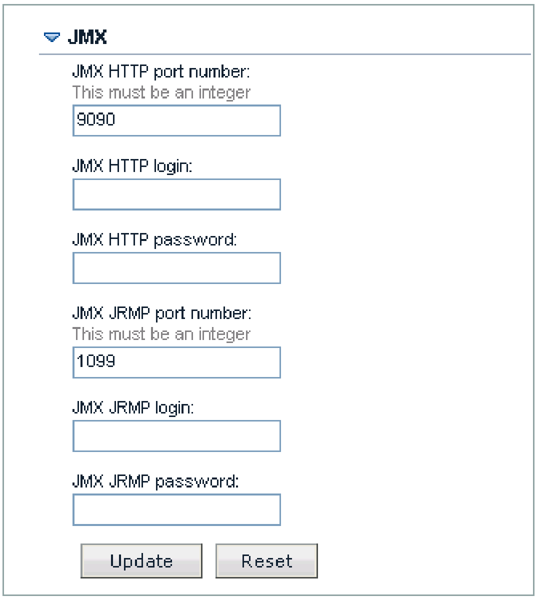
  Specify the port number of the HTTP adaptor for JMX, if the HTTP interface for JMX is to be enabled.

- **JMX HTTP login**

  Specify the login user name for the HTTP adaptor for JMX, if the HTTP interface for JMX is to be enabled.

- **JMX HTTP password**

  Specify the password for the HTTP adaptor for JMX, if the HTTP interface for JMX is to be enabled.



JMX

JMX HTTP port number:
This must be an integer
9090

JMX HTTP login:

JMX HTTP password:

JMX JRMP port number:
This must be an integer
1099

JMX JRMP login:

JMX JRMP password:

JMX

- JMX JRMP port number

  Specify the port number of the JRMP adaptor for JMX, if the JRMP interface for JMX is to be enabled.

- JMX JRMP login

  Specify the login user name for the JRMP adaptor for JMX, if the JRMP interface for JMX is to be enabled.

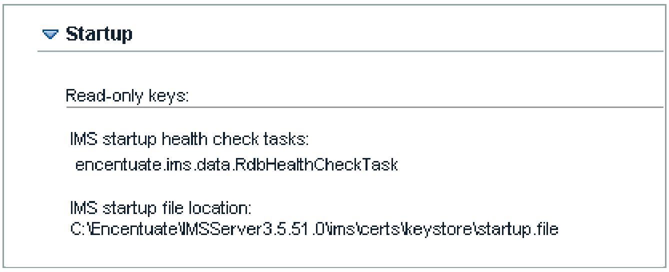
- JMX JRMP password

  Specify the password for the JRMP adaptor for JMX, if the JRMP interface for JMX is to be enabled.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Startup



Startup

Read-only keys:

IMS startup health check tasks:
encentuate.ims.data.RdbHealthCheckTask

IMS startup file location:
C:\Encentuate\IMSServer3.5.51.0\ims\certs\keystore\startup.file

Startup

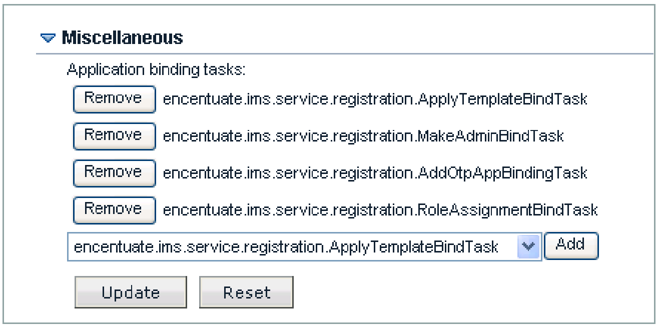
- IMS startup health check tasks

  A list of health checking tasks that are executed when IMS starts.

- IMS startup file

  The file that is needed by IMS to Start-Up.

Miscellaneous



Miscellaneous

Application binding tasks:

encentuate.ims.service.registration.ApplyTemplateBindTask

encentuate.ims.service.registration.MakeAdminBindTask

encentuate.ims.service.registration.AddOtpAppBindingTask

encentuate.ims.service.registration.RoleAssignmentBindTask

encentuate.ims.service.registration.ApplyTemplateBindTask

Miscellaneous

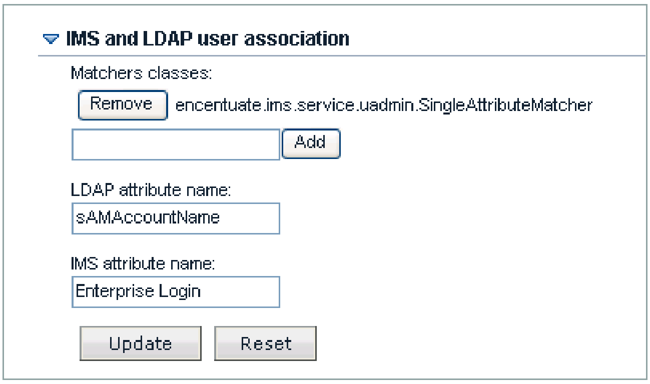
- Application binding tasks

  The classnames of the tasks that must be performed when application binding occurs.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

IMS and LDAP user association



IMS and LDAP user association

Matchers classes:

encentuate.ims.service.uadmin.SingleAttributeMatcher

LDAP attribute name:

sAMAccountName

IMS attribute name:

Enterprise Login

IMS and LDAP user association

- Matchers classes

  Fully qualified class names of the matchers in the order they will be used to associate an IMS user and an LDAP user.

- LDAP attribute name

  Name of the LDAP attribute which will be used to associate an IMS user and an LDAP user (such as sAMAccountName).

- IMS attribute name

  Name of the IMS attribute which will be used to associate an IMS user and an LDAP user (such as Enterprise Login).

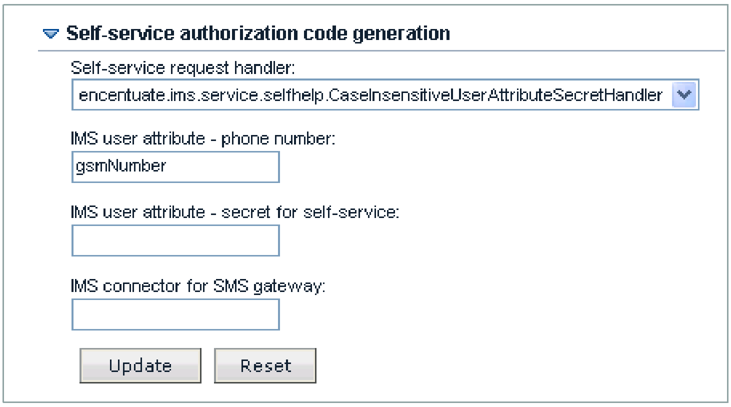
Self-service authentication code generation

- Self-service request handler

  Fully qualified class name that implements AuthCodeRequestHandler interface. this handler must be specified if the self-service feature is enabled.

- IMS user attribute - phone number

  Name of the IMS user attribute that stores users' phone numbers (for example, gsmNumber).



Self-service authorization code generation

Self-service request handler:
encentuate.ims.service.selfhelp.CaseInsensitiveUserAttributeSecretHandler

IMS user attribute - phone number:
gsmNumber

IMS user attribute - secret for self-service:

IMS connector for SMS gateway:

Self-service authorization code generation

- IMS user attribute - secret for self-service

  Name of the IMS user attribute whose value is used as secret in requests for authorization code.

- IMS connector for SMS gateway

  Name of one IMS connector that communicates with an SMS gateway. This configuration is required if IMS needs to deliver authorization code through SMS.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Data source

To configure data source, select *Advanced Settings >> Data Source* from the IMS Configuration Utility navigation panel.

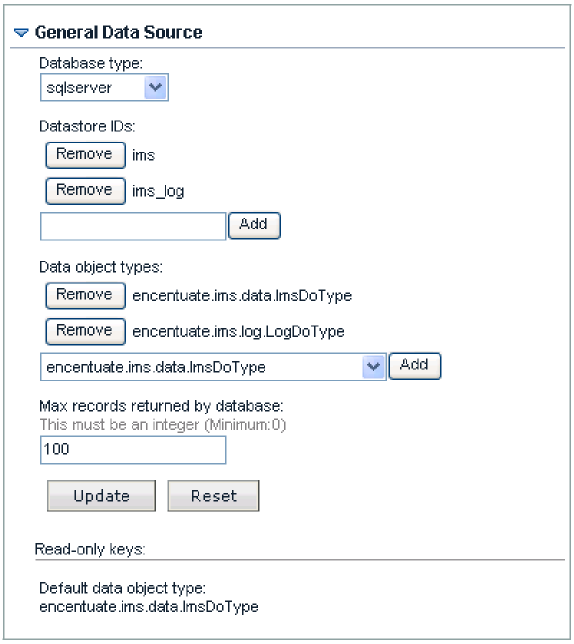
General data source

- Database type

  The type of database (MSSQL Server, Oracle).

- Datastore IDs

  Each value of ds.do_types must have a corresponding value here. It defines the data source parameters used for the associated ds.do_type. The associated group of parameters will have the ID in its name. For example ds.ims.rdb.*. If any ds.do_type share the same data source ID, the two groups of DOs will share the same connection pool.



General Data Source

Database type:
sqlserver

Datastore IDs:
Remove ims
Remove ims_log

Data object types:
Remove encentuate.ims.data.ImsDoType
Remove encentuate.ims.log.LogDoType
encentuate.ims.data.ImsDoType

Max records returned by database:
This must be an integer (Minimum:0)
100

Read-only keys:

Default data object type:
encentuate.ims.data.ImsDoType

General Date Source

- Default data object type

  This is the default ds.do_type (ds stands for data store and do is data object) if no value is specified during a request for a connection, and if data source parameters for other ds.do_types are not found.

- **Data object types**

  The fully qualified classname of a class that contains the types of a logical group of DOs. There can be multiple values for this tag. Each value identifies a logical group of DO, each of which can use a different connection pool (such as different data source).

- **Max records returned by database**

  This specifies the maximum number of results that will be shown on the Encentuate IMS Server user interface when a search is performed. By default the value is set to 25.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

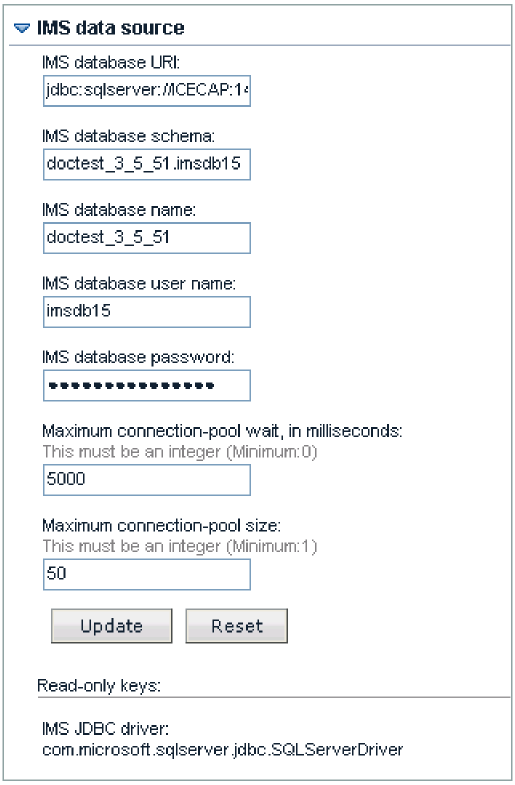
IMS data source

- **IMS database URI**

  The Uniform Resource Identifier (URI) of the RDB server.

- **IMS database schema**

  The schema of the database tables for do_type.



IMS data source

IMS database URI:
jdbc:sqlserver://ICECAP:1

IMS database schema:
doctest_3_5_51.imsdb15

IMS database name:
doctest_3_5_51

IMS database user name:
imsdb15

IMS database password:
•••••••••••••••

Maximum connection-pool wait, in milliseconds:
This must be an integer (Minimum:0)
5000

Maximum connection-pool size:
This must be an integer (Minimum:1)
50

Read-only keys:

IMS JDBC driver:
com.microsoft.sqlserver.jdbc.SQLServerDriver

IMS data source

- IMS database name

  The name of the IMS database.

- IMS JDBC driver

  The fully qualified classname of the JDBC driver.

- IMS database user name

  The user name that can be used to log on to the database.

- IMS database password

  The corresponding password for the user name that can be used to log on to the database. When run for the first time, it is replaced by a fixed string with the encrypted value written in the ciphertext section.

- Maximum connection-pool wait in milliseconds

  How long to wait (in milliseconds) for a RDB connection when no connections are available.

- Maximum connection-pool size

  Maximum number of connections allowed in connection pooling.

Click Update to save the new settings.

Click Reset to discard changes.

Log data source

- IMS log database URI

  The Uniform Resource Identifier (URI) of the RDB server.

- IMS log database schema

  The schema of the database tables for do_type.

- IMS log database name

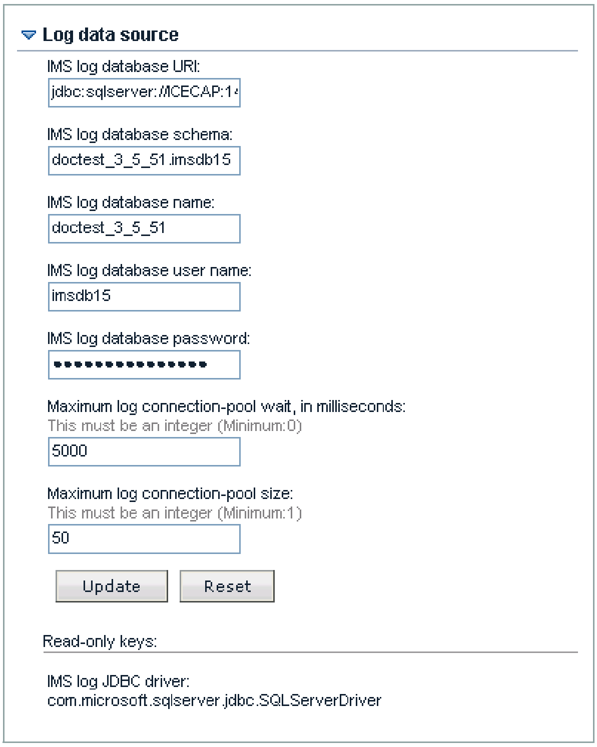
  The name of the IMS log database.

- IMS log JDBC driver

  The fully qualified classname of Java Database Connectivity (JDBC) driver.

- IMS log database user name

  The user name to log onto the log database with.



Log data source

IMS log database URI:
jdbc:sqlserver://CECAP:1

IMS log database schema:
doctest_3_5_51.imsdb15

IMS log database name:
doctest_3_5_51

IMS log database user name:
imsdb15

IMS log database password:
•••••••••••••••

Maximum log connection-pool wait, in milliseconds:
This must be an integer (Minimum:0)
5000

Maximum log connection-pool size:
This must be an integer (Minimum:1)
50

Read-only keys:

IMS log JDBC driver:
com.microsoft.sqlserver.jdbc.SQLServerDriver

Log data source

- IMS log database password

  The corresponding password for the user name that can be used to log on to the database. When run for the first time, it is replaced by a fixed string with the encrypted value written in the ciphertext section.

- Maximum log connection-pool wait in milliseconds

  How long to wait (in milliseconds) for an ims_log connection before declaring that no connections are available.

- Maximum log connection-pool size

  The maximum size of the log connection pool.

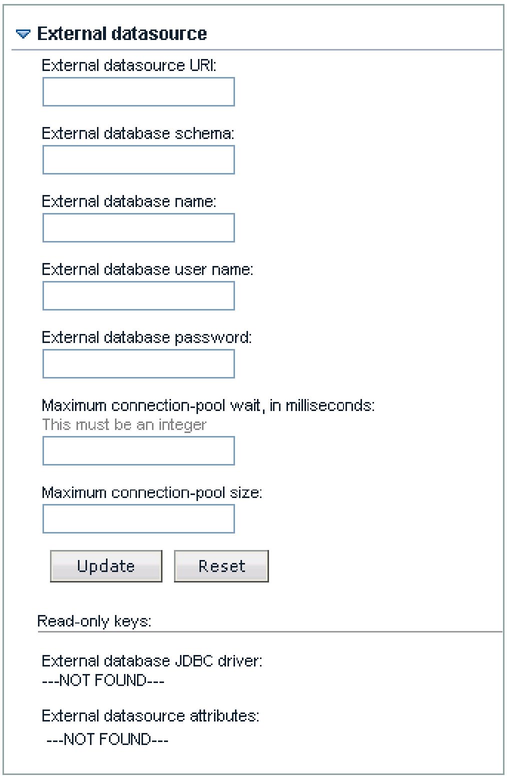
Click **Update** to save the new settings.

Click **Reset** to discard changes.

External data source

- External datasource URI

  The Uniform Resource Identifier (URI) of the external datasource.



External datasource

External datasource URI:

External database schema:

External database name:

External database user name:

External database password:

Maximum connection-pool wait, in milliseconds:
This must be an integer

Maximum connection-pool size:

Read-only keys:

External database JDBC driver:
---NOT FOUND---

External datasource attributes:
---NOT FOUND---

External datasource

- **External database scheme**

  The schema of the database tables for do_type.

- **External database name**

  The name of the IMS log database.

- **External database JDBC driver**

  The fully qualified classname of Java Database Connectivity (JDBC) driver.

- **External database user name**

  The user name to log onto the log database with.

- **External database password**

  The corresponding password for the user name that can be used to log on to the database. When run for the first time, it is replaced by a fixed string with the encrypted value written in the ciphertext section.

- **Maximum connection-pool wait in milliseconds**

  How long to wait (in milliseconds) for a external connection before declaring that no connections are available.

- **Maximum connection-pool size**

  The maximum size of the log connection pool.

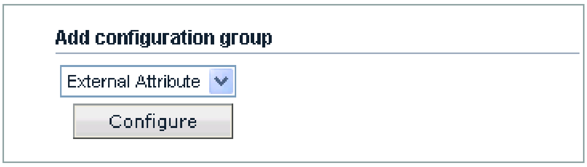
- **External datasource attributes**

  Attribute names that are used in IMS to lookup their value in external datasource.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Add configuration group

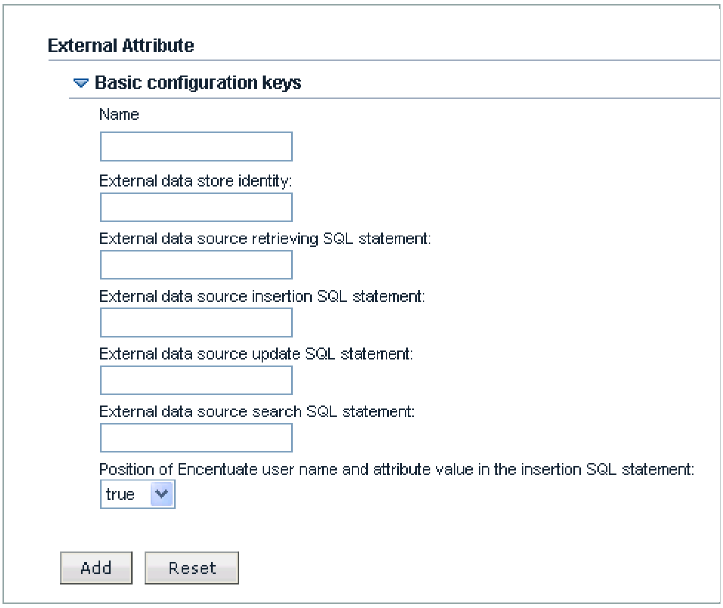


Add configuration group

External Attribute

Add configuration group

To add a configuration group, select a group from the drop-down list and click **Configure**.



External Attribute

Basic configuration keys

Name

External data store identity:

External data source retrieving SQL statement:

External data source insertion SQL statement:

External data source update SQL statement:

External data source search SQL statement:

Position of Encentuate user name and attribute value in the insertion SQL statement:

true

External Attribute - Basic configuration keys

- **External data store identity**

  One of the data store identities that is defined in the Data Store section.

- External data source retrieving SQL statement

  SQL statement to retrieve the attribute value from external datasource.

- External data source insertion SQL statement

  SQL statement to insert the attribute value from external datasource.

- External data source update SQL statement

  SQL statement to update the attribute value from external datasource.

- External data source search SQL statement

  SQL statement to search for enterprise identities with certain attribute values from the external datasource.

- The position of Encentuate user name and attribute value in the insertion SQL statement

  The position of enterprise ID and attribute value in the insertion SQL statement.

Application connectors

For information about the available connectors, see IMS Server housekeeping.

Click **Update** to save the new settings.

Click **Reset** to discard changes.

Message connectors

To configure message connector, select *Advanced Settings >> Message Connectors* from the IMS Configuration Utility navigation panel. In **Add Configuration Group**, select a message connector from the drop-down list and click **Configure**.

SMPP Messaging Connector

Basic configuration keys

- Message Connector Name

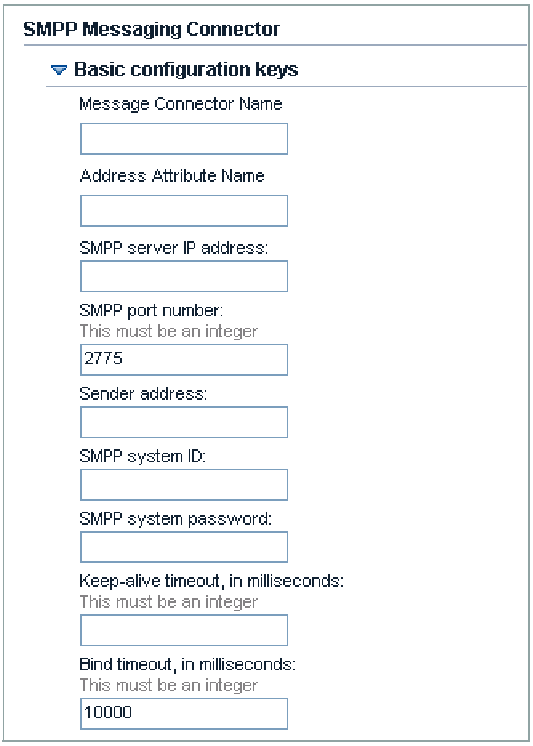
  The display name of the web-based SMS connector.

- Address Attribute Name

  A name to describe the address attribute.

- SMPP server IP address

  The IP address of the SMPP server.



SMPP Messaging Connector

Basic configuration keys

Message Connector Name

Address Attribute Name

SMPP server IP address:

SMPP port number:
This must be an integer
2775

Sender address:

SMPP system ID:

SMPP system password:

Keep-alive timeout, in milliseconds:
This must be an integer

Bind timeout, in milliseconds:
This must be an integer
10000

SMPP Messaging Connector - Basic configuration keys

- SMPP port number

  Specifies the TCP/IP port on the SMPP server to which the gateway should connect.

- Sender address

  Specifies the default sender address to apply to outbound messages.

- SMPP system ID

  Specifies the user name for the gateway to use when connecting to the SMPP server.

- SMPP system password

  Specifies the password for the gateway to use when connecting to the SMPP server.

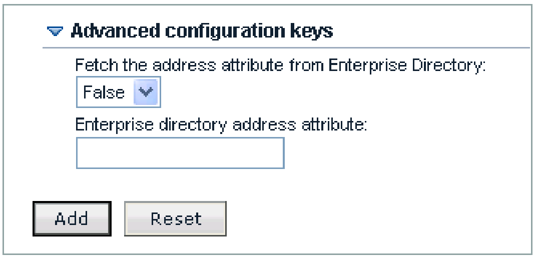
- Keep-alive timeout

  Specifies how long a network connection should wait for a new request before closing.

- Bind timeout

  Specifies the maximum amount of time in seconds that a client spends attempting to bind to the domain.

Advanced configuration keys



Advanced configuration keys

Fetch the address attribute from Enterprise Directory:

False

Enterprise directory address attribute:

Advanced configuration keys

- Fetch the address attribute from Enterprise Directory?

  Specifies whether the address attribute used by this messaging connector should be fetched from the Enterprise Directory. If set to false, the address attribute (specified by Address Attribute Name) is fetched from the IMS database.

  Limitations:

  - If set to true, performance will be degraded as each MAC issuance makes a call to the Enterprise Directory.
  - To support fetching of multi-valued attributes (like “memberOf”), the ADSI connector should be used for configuring the Enterprise Directory (see Encentuate IAM Administrator Guide for details).

- Enterprise Directory address attribute

  This specifies the name of the attribute to be looked up from the Enterprise Directory (AD or LDAP server). This needs to be set only if “Fetch the address attribute from Enterprise Directory?” is set to “True”. If this attribute specifies a phone number, it should be of the format “CountryCode-AreaCode-PhoneNumber”, for example, “1-650-4136800”, “65--64735110”.

SMTP Messaging Connector

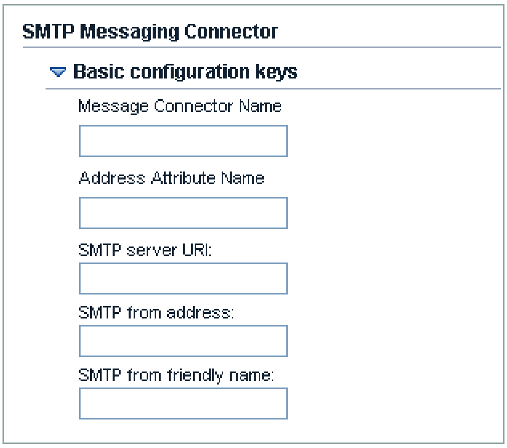
Basic configuration keys

- Message connector name

  The display name of the web-based SMS connector.

- Address attribute name

  A name to describe the address attribute.



SMTP Messaging Connector

Basic configuration keys

Message Connector Name

Address Attribute Name

SMTP server URI:

SMTP from address:

SMTP from friendly name:

SMTP Messaging Connector - Basic configuration keys

- SMTP server URI

  The URI of the SMTP Server (For example: mail.mycompany.com).

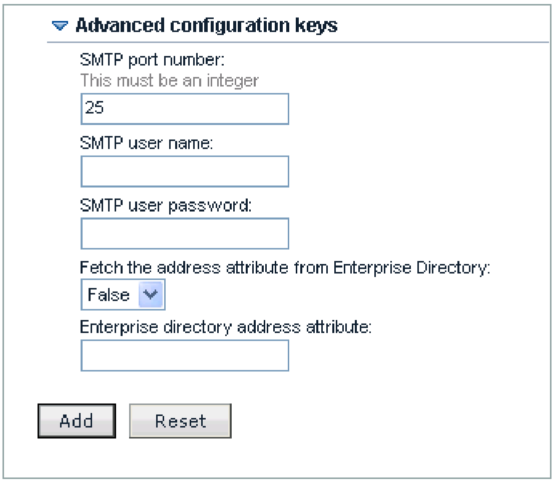
- SMTP from address

  The address from which electronic mails are sent.

- SMTP from friendly name

  A friendly name to be used in place of the e-mail address.

Advanced configuration keys



Advanced configuration keys

SMTP port number:
This must be an integer
25

SMTP user name:

SMTP user password:

Fetch the address attribute from Enterprise Directory:
False

Enterprise directory address attribute:

Advanced configuration keys

- SMTP port number

  SMTP server port number.

- SMTP user name

  The user name which is used for SMTP authentication.

- SMTP user password

  The password which is used for SMTP authentication.

  The user name which is used for SMTP authentication.

- Fetch the address attribute from Enterprise Directory?

  Specifies whether the address attribute used by this messaging connector should be fetched from the Enterprise Directory. If set to false, the address attribute (specified by Address Attribute Name) is fetched from the IMS database.

  Limitations:

  - If set to true, performance will be degraded as each MAC issuance makes a call to the Enterprise Directory.
  - To support fetching of multi-valued attributes (like "memberOf"), the ADSI connector should be used for configuring the Enterprise Directory (see Encentuate IAM Administrator Guide for details).

- Enterprise Directory address attribute

  This specifies the name of the attribute to be looked up from the Enterprise Directory (AD or LDAP server). This needs to be set only if "Fetch the address attribute from Enterprise Directory?" is set to "True". If this attribute specifies a phone number, it should be of the format "CountryCode-AreaCode-PhoneNumber", for example, "1-650-4136800", "65--64735110".

Web-based SMS Connector

Basic configuration keys

- Message connector name

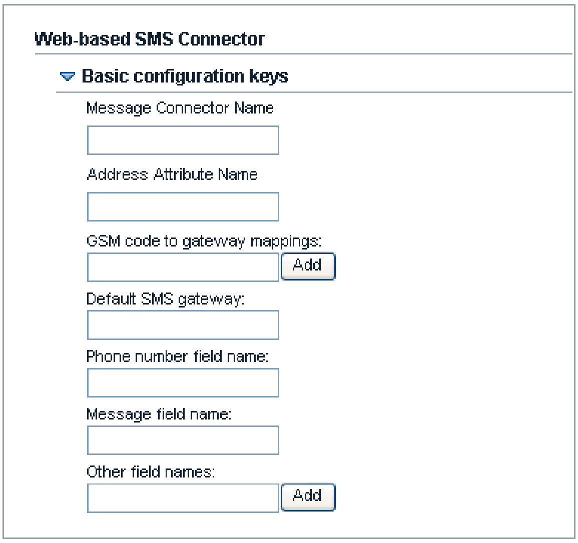
  The display name of the web-based SMS connector.

- Address attribute name

  A name to describe the address attribute.

- GSM Code to gateway mappings

  Mappings of GSM codes to the corresponding gateway IP address or hostname (For example: 65,127.0.0.1).



Web based SMS Connector - Basic configuration keys

- Default SMS gateway

  The SMS gateway IP address or hostname that will be used if the current GSM code does not match any of the GSM code to gateway mappings.

- Phone number field

  Name of the phone number field on the target web-form used to send the SMS.

- Message field

  Name of the message field on the target web-form used to send the SMS.

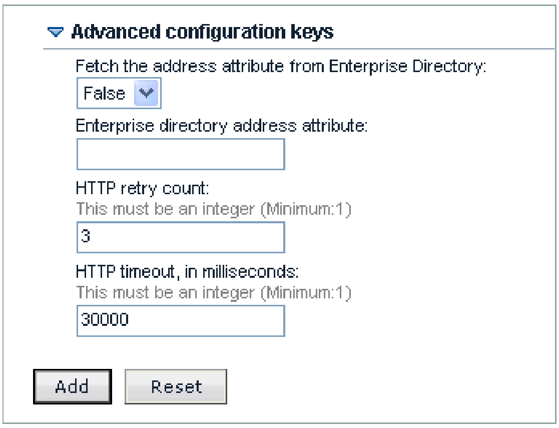
- Other fields

  Comma-separated name-value mappings of other fields to be sent to the target web-form (For example: group, executives).

Advanced configuration keys

- Fetch the address attribute from Enterprise Directory?

  Specifies whether the address attribute used by this messaging connector should be fetched from the Enterprise Directory. If set to false, the address attribute (specified by Address Attribute Name) is fetched from the IMS database.



Advanced configuration keys

Fetch the address attribute from Enterprise Directory: False

Enterprise directory address attribute:

HTTP retry count: This must be an integer (Minimum:1) 3

HTTP timeout, in milliseconds: This must be an integer (Minimum:1) 30000

Advanced configuration keys

Limitations:

- If set to true, performance will be degraded as each MAC issuance makes a call to the Enterprise Directory.
- To support fetching of multi-valued attributes (like "memberOf"), the ADSI connector should be used for configuring the Enterprise Directory (see Encentuate IAM Administrator Guide for details).

- Enterprise directory address attribute

  This specifies the name of the attribute to be looked up from the Enterprise Directory (AD or LDAP server). This needs to be set only if "Fetch the address attribute from Enterprise Directory?" is set to "True". If this attribute specifies a phone number, it should be of the format "CountryCode-AreaCode-Phone-Number", for example, "1-650-4136800", "65--64735110".

- HTTP retry count

  This specifies the number of times to retry establishing an HTTP. connection when the connection fails on the first try.

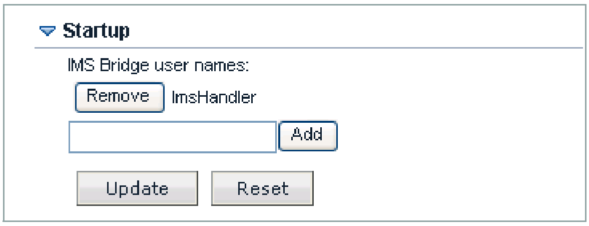
- HTTP timeout (milliseconds)

  This specifies the amount of time, in milliseconds, to wait for a server response. If you have a slow network connection, increase the value of this option.

IMS bridges

To configure IMS bridges, select *Advanced Settings >> IMS Bridges* from the IMS Configuration Utility navigation panel.

Startup



Startup

IMS Bridge user names:

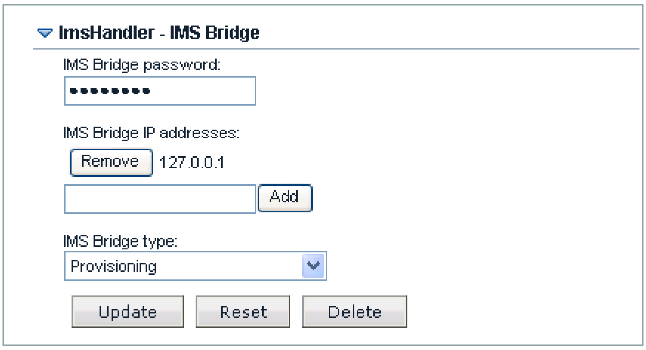
Remove ImsHandler

Startup

IMS Bridge user names

Names for authenticating the IMS Bridge.

IMS Handler-IMS Bridge



ImsHandler - IMS Bridge

IMS Bridge password: ••••••••

IMS Bridge IP addresses:

Remove 127.0.0.1

IMS Bridge type: Provisioning

ImsHandler - IMS Bridge

- IMS Bridge password

  The password used to authenticate the IMS Bridge.

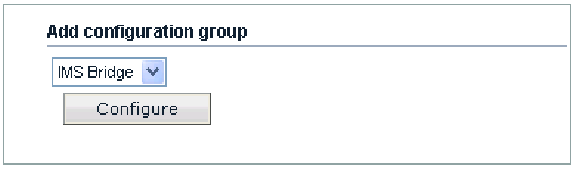
- IMS Bridge IP addresses

  The IP addresses from which the IMS Bridge can access the IMS Server.

- IMS Bridge type

  The role which will be assigned to the IMS Bridge when it logs on.

Add Configuration Group



Add configuration group

IMS Bridge

Add configuration group

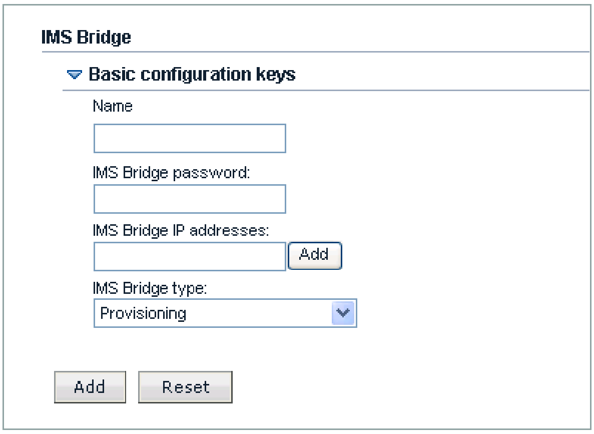
IMS Bridge Configuration

- Name

  Name used to authenticate the IMS Bridge.

- IMS Bridge password

  The password used to authenticate the IMS Bridge.



IMS Bridge type: Provisioning

IMS Bridge - Basic configuration keys

- IMS Bridge IP addresses

  The IP addresses from which the IMS Bridge can access the IMS Server.

- IMS Bridge type

  The role which will be assigned to the IMS Bridge when it logs on.

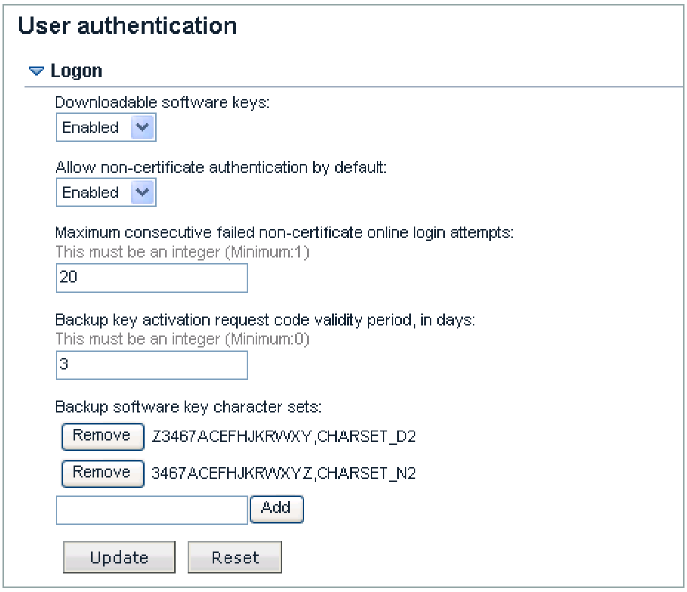
User authentication

To configure user authentication, select *Advanced Settings >> User Authentication* from the IMS Configuration Utility navigation panel.

Logon

- Downloadable software keys

  System wide policy to decide if the user can create downloadable software keys.



User authentication

Logon

Downloadable software keys:
Enabled

Allow non-certificate authentication by default:
Enabled

Maximum consecutive failed non-certificate online login attempts:
This must be an integer (Minimum:1)
20

Backup key activation request code validity period, in days:
This must be an integer (Minimum:0)
3

Backup software key character sets:
Z3467ACEFHJKRWXY,CHARSET_D2
3467ACEFHJKRWXYZ,CHARSET_N2

User authentication - Logon

- **Allow non-certificate authentication by default**

  If all users are allowed to access non-certificate based authentication by default. If there is no user based access control policy for non-certificate based authentication, this system wide policy will be enforced. If this key is not specified, no users are allowed by default and IMS system Administrator has to give permission to each user explicitly.

- **Max consecutive failed non-certificate online login attempts**

  The maximum number of consecutive failures before the user is locked out, which means logging on to IMS using non-certificate based authentication will not be allowed.

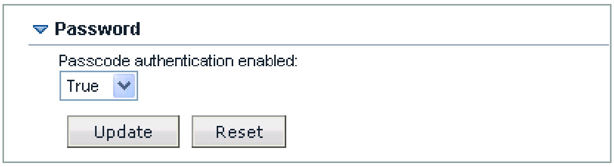
- **Backup key activation request code validity period in days**

  The number of days for which the Activation Request Code will be considered as valid after it has been generated.

- **The backup software key character sets**

  The Character sets that can be supported by the IMS Server. The value is of the form character_set, N2 or character_set, D2 depending upon whether the deployment contains AA which have different BSK Secrets on every computer. Example value: Z3467ALEQHJKRWXY,CHARSET_D2. Please note that all the character sets should be positionally unambiguous.

Password


Password

Passcode authentication enabled:

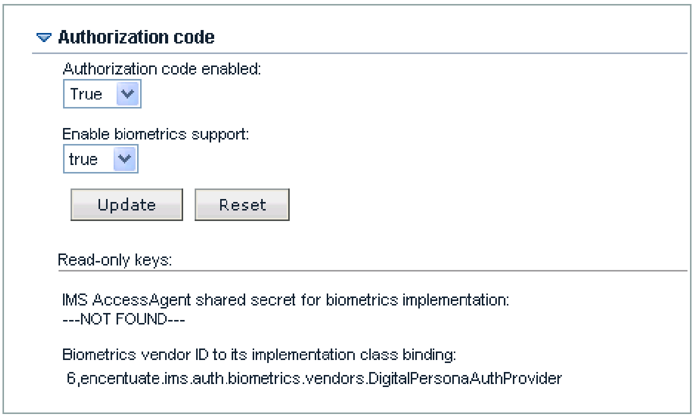
True

Password

- **Password authentication enabled**

  Specifies whether password authentication is allowed by the IMS Server.

Authorization code


Authorization code

Authorization code enabled:

True

Enable biometrics support:

true

Read-only keys:

IMS AccessAgent shared secret for biometrics implementation:
---NOT FOUND---

Biometrics vendor ID to its implementation class binding:
6,encentuate.ims.auth.biometrics.vendors.DigitalPersonaAuthProvider

Authorization code

- **Authorization code enabled**

  Specifies whether authorization code authentication is allowed by the IMS Server.

- **Enable biometrics support**

  This value is a switch for enabling / disabling the biometrics support.

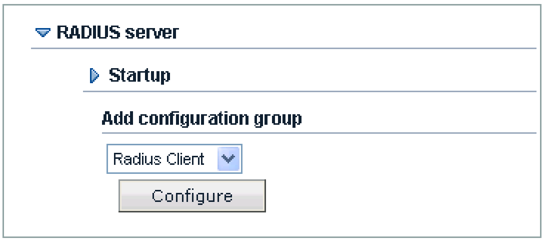
- **IMS AccessAgent shared secret for biometrics implementation.**

  This value is a secret shared between the IMS and AA and is required for the biometrics implementation.

- **Biometrics vendor ID to its implementation class binding.**

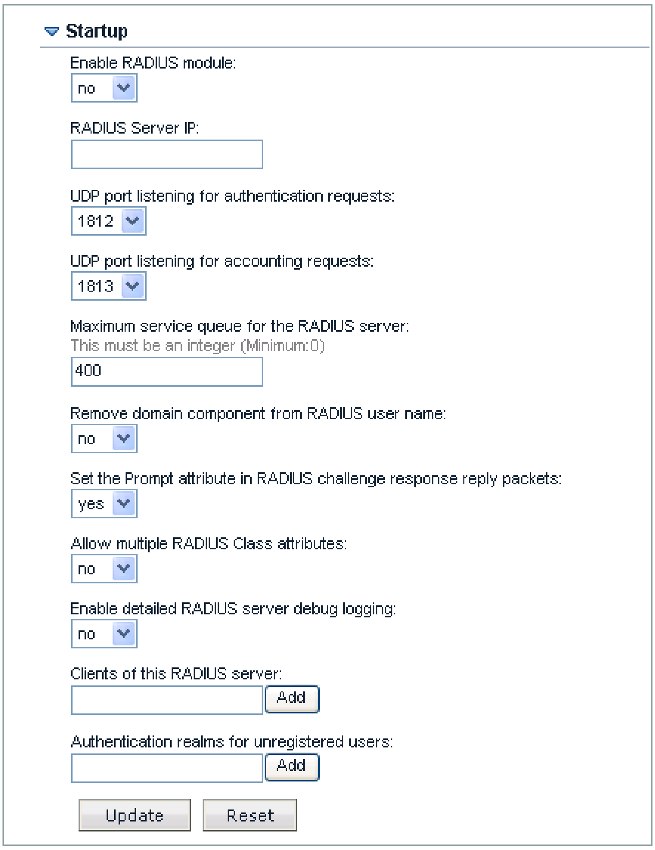
  This key specifies a set a bindings between the biometrics vendors supported by the IMS, and the classes which implement the vendor specific algorithms.

RADIUS Server



RADIUS server

Startup



Startup

Enable RADIUS module: no

RADIUS Server IP:

UDP port listening for authentication requests: 1812

UDP port listening for accounting requests: 1813

Maximum service queue for the RADIUS server:
This must be an integer (Minimum:0)
400

Remove domain component from RADIUS user name: no

Set the Prompt attribute in RADIUS challenge response reply packets: yes

Allow multiple RADIUS Class attributes: no

Enable detailed RADIUS server debug logging: no

Clients of this RADIUS server:

Authentication realms for unregistered users:

Startup

- **Enable RADIUS module**

  Turn on/off the RADIUS module.

- **Radius Server IP**

  IP address of the RADIUS server.

- UDP port listening for authentication requests

  Port that the server listens on for RADIUS Authentication requests. The default value is 1812.

- UDP port listening for accounting requests

  Port that the server listens on for RADIUS Accounting requests. The default value is 1813.

- Maximum service queue for the Radius server

  Specifies the maximum service queue before the system regards the Radius server as unavailable.

- Remove domain component from RADIUS user name

  Strip the domain component from the user name.

- Set the Prompt attribute in RADIUS challenge response reply packets

  Set the Prompt attribute in RADIUS challenge response reply packets. Some VPNs (notably Checkpoint) will not allow RADIUS packets with the Prompt attribute set, while others (such as Aventail) require it to be set.

- Allow multiple RADIUS Class attributes

  Enabling this will allow the user's LDAP attribute to be correctly sent as multiple RADIUS Class attributes. However, for VPNs that can handle only a single RADIUS Class attribute, this feature will have to be disabled.

- Enable detailed RADIUS server debug logging

  This may affect performance and privacy, so enable only when needed for troubleshooting/debugging.

- Clients of this RADIUS server

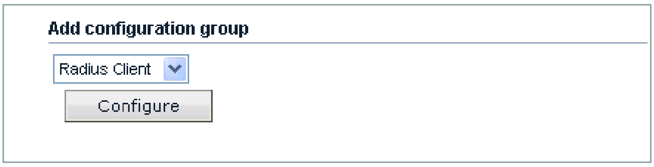
  List of RADIUS clients, IP address/FQDNs are specified in the key radius.client.$friendlyName.address.

- Authentication realms for unregistered users

  List of Realms that non IMS users are authenticated against. An LDAP type realm can be used to retrieve memberOf and other user attributes for registered ims users if the VPN user ID and the ldap user id match.

- Add configuration group

  Click the Configure button to open the Radius Client configuration page.



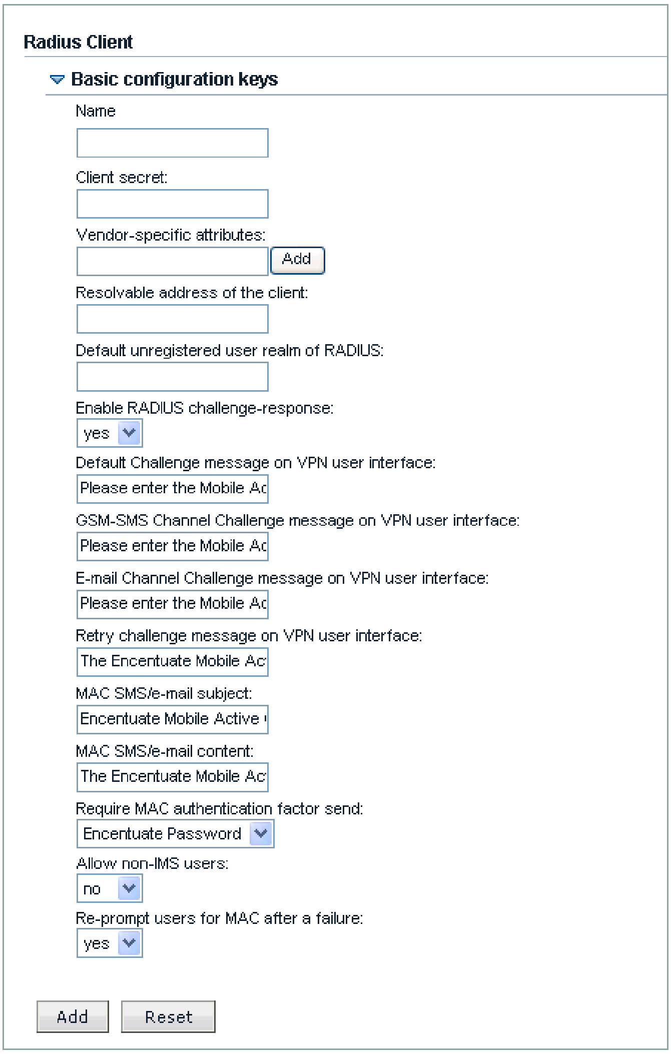
Add configuration group

Radius Client

Add configuration group

Radius Client

Basic configuration keys



Radius Client

Basic configuration keys

Name

Client secret:

Vendor-specific attributes:

Resolvable address of the client:

Default unregistered user realm of RADIUS:

Enable RADIUS challenge-response: yes

Default Challenge message on VPN user interface: Please enter the Mobile Ac

GSM-SMS Channel Challenge message on VPN user interface: Please enter the Mobile Ac

E-mail Channel Challenge message on VPN user interface: Please enter the Mobile Ac

Retry challenge message on VPN user interface: The Encentuate Mobile Ac

MAC SMS/e-mail subject: Encentuate Mobile Active

MAC SMS/e-mail content: The Encentuate Mobile Ac

Require MAC authentication factor send: Encentuate Password

Allow non-IMS users: no

Re-prompt users for MAC after a failure: yes

Radius client - Basic configuration keys

- Name

The name of the new client.

- Client secret

  Shared secret used to encrypt communication between the RADIUS client and server.

- Vendor-specific attributes

  RADIUS attributes returned on successful authentication.

- Resolvable address of the client

  IP address or FQDN of the host listed as RADIUS client.

- Default unregistered user realm of RADIUS

  Name of the default unregistered user realm for this RADIUS server

- Enable RADIUS challenge-response

  Enable RADIUS Challenge-Response for this VPN server

- Default Challenge message on VPN user interface

  The RADIUS Challenge message that the user sees on the VPN user interface

- GSM-SMS Channel Challenge message on VPN user interface

  The RADIUS challenge message that the user sees on the VPN user interface if the MAC is sent using an SMS gateway (such as via a Web-based SMS message connector). This step is only required if MAC is enabled.

- Email Channel Challenge message on VPN user interface

  The RADIUS challenge message that the user sees on the VPN user interface if the MAC is sent using an email gateway (such as via an Email message connector). This step is only required if MAC is enabled.

- Retry Channel Challenge message on VPN user interface

  The RADIUS Challenge message that the user seen on the VPN UI.

- Subject of MAC SMS or e-mail

  The template of the SMS or EMail message the user receives with the MAC in it.

- Body of MAC SMS or e-mail

  The template of the SMS or EMail message the user receives with the MAC in it.

- Allow non-IMS users

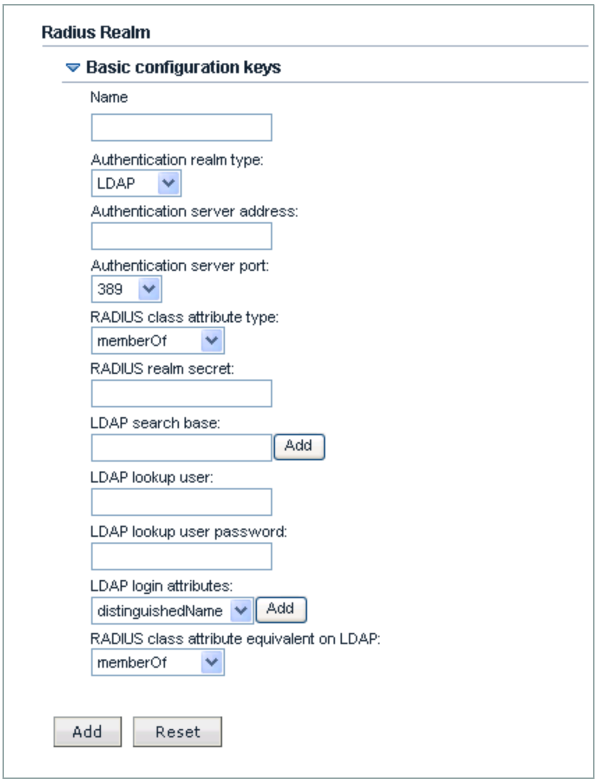
  Select No. This prevents unregistered users from authenticating using this VPN server.

- Re-prompt users for MAC after a failure

  Prompt users to re-enter a MAC if it is entered incorrectly. The user will be prompted until the account is locked.

RADIUS Realm

Basic configuration keys



Radius Realm

Basic configuration keys

Name:

Authentication realm type: LDAP

Authentication server address:

Authentication server port: 389

RADIUS class attribute type: memberOf

RADIUS realm secret:

LDAP search base:

LDAP lookup user:

LDAP lookup user password:

LDAP login attributes: distinguishedName

RADIUS class attribute equivalent on LDAP: memberOf

Radius Realm - Basic configuration keys

- Name

  Name of the new RADIUS realm.

- Authentication realm type

  The type of authentication realm.

- Authentication server address

  Address of the principal authentication server of this realm.

- Authentication server port

  The port on which the authentication server listens to for authentication requests.

- RADIUS class attribute type

  The type of RADIUS Class attribute that this realm returns.

- RADIUS realm secret

  The shared secret between IMS-RADIUS and this RADIUS realm

- LDAP search base

  Distinguished name of the LDAP objects used as the roots for any LDAP search.

- LDAP lookup user

  The user with permissions to search, retrieve LDAP attributes.

- LDAP lookup user password

  The password of the RADIUS-LDAP lookup user.

- LDAP login attributes

  LDAP login attributes that are searched for when the user logs in.

- RADIUS class attribute equivalent on LDAP

  The LDAP attribute that will be returned to the RADIUS client as the "Class" standard RADIUS attribute.

Deprovisioning

To perform deprovisioning tasks, select *Advanced Settings >> Deprovisioning* from the IMS Configuration Utility navigation panel.

- Deprovisioning access password

  The shared secret between the client and the server for deprovisioning calls.

- Allowed deprovisioning client IPs

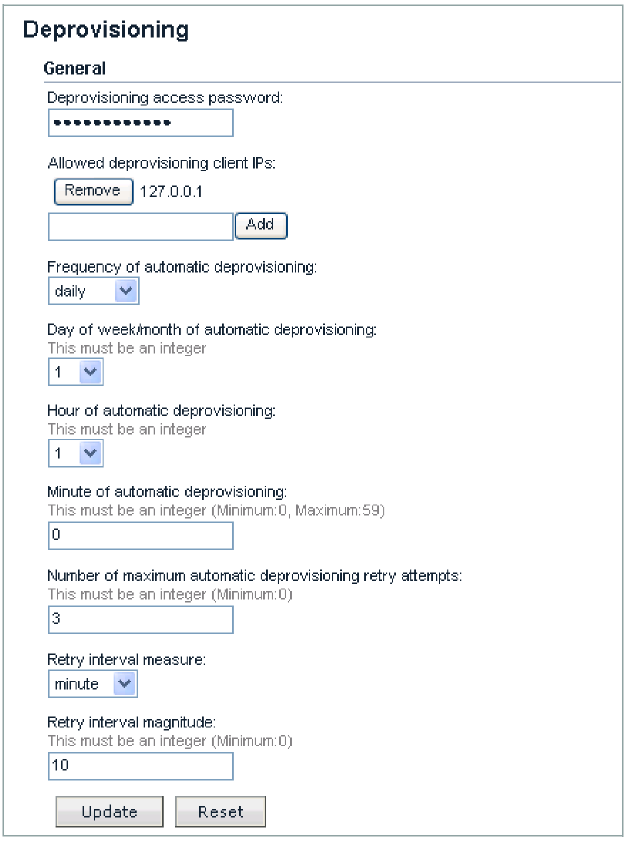
  The list of client IPs that are allowed to call the deprovisioning SOAP service.

- Frequency of automatic deprovisioning

  The frequency which the automatic deprovisioning task should run.

- Day of week/month of automatic deprovisioning

  This value only has meaning if the frequency is set to weekly or monthly in which case it means the day of the week or month respectively that the automatic deprovisioning task should run.



Deprovisioning

General

Deprovisioning access password: ●●●●●●●●●●●●

Allowed deprovisioning client IPs:

127.0.0.1

Frequency of automatic deprovisioning: daily

Day of week/month of automatic deprovisioning:
This must be an integer
1

Hour of automatic deprovisioning:
This must be an integer
1

Minute of automatic deprovisioning:
This must be an integer (Minimum:0, Maximum:59)
0

Number of maximum automatic deprovisioning retry attempts:
This must be an integer (Minimum:0)
3

Retry interval measure: minute

Retry interval magnitude:
This must be an integer (Minimum:0)
10

Deprovisioning - General

- Hour of automatic deprovisioning

  The hour at which the automatic deprovisioning task should run.

- Minute of automatic deprovisioning

  The minute at which the automatic deprovisioning task should run.

- Number of maximum automatic deprovisioning retry attempts

  The number of times the automatic deprovisioning task will be retried if it fails.

- Retry interval measure

  The measure of the interval between retry attempts.

- Retry interval magnitude

  The magnitude of the interval between automatic deprovisioning retry attempts.

Glossary and Abbreviations

AccessAdmin

The management console used by individuals with the Administrator Role and/ or the Helpdesk Role to administer IMS Server, and to manage users and policies.

AccessAgent

AccessAgent, or AA, is the client software that manages the user's identity, enabling sign-on/sign-off automation and authentication management.

AccessAssistant

The web-based interface used to provide password self-help for users to obtain the latest credentials to logon to their applications.

AccessProfiles

Short, structured XML files that enable single sign-on/sign-off automation for applications. AccessStudio can be used to generate AccessProfiles.

AccessStudio

The interface used to create AccessProfiles required to support end-point automation, including single sign-on, single sign-off, and customizable audit tracking.

AD

Microsoft Active Directory

ADAM

Active Directory Application Mode

ADSI

Active Directory Service Interfaces

API

Application Programming Interface

application

In AccessStudio, it refers to the system that provides the user interface for reading/ entering the authentication credentials.

application group

A set of applications that share the same directory. In other words, a user can logon to any of the applications in the application group using the same user name.

application policy

Collections of policies and attributes governing access to applications.

authentication factor

The different devices, biometrics, or secrets required as credentials for validating digital identities (e.g., passwords, Encentuate USB Key, RFID, biometrics, and one-time password tokens).

authentication service

Verifies the validity of an account; Applications authenticate against their own user store or against a corporate directory.

authorization code

An alphanumeric code generated by an Encentuate Helpdesk user for administrative functions, such as password resets or authentication factors for the Wallet; may be used one or more times based on policy.

biometrics

The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice or handwriting.

CA

Certificate Authority

CAPI

Microsoft Cryptography API

CLT

Command Line Tool

CSN

Card Serial Number (for Mifare RFID cards)

DB

Database

DLL

Dynamic Link Library

DNS

Domain Name Service

EnGINA

Encentuate GINA, which replaces the Microsoft GINA. EnGINA provides a user interface that is tightly integrated with authentication factors and provide password resets and second factor bypass options.

Enterprise Access Security (EAS)

A technology that enables enterprises to simplify, strengthen and track access to digital assets and physical infrastructure.

Enterprise Single Sign-On (ESSO)

A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials (such as a password). Many ESSO products use sign-on automation technologies to achieve SSO—users logon to the sign-on automation system and the system logs on the user to all other applications.

identity wallet

A secured data store for a user's access credentials and related information (including user IDs, passwords, certificates, encryption keys). The Wallet is an identity wallet.

GINA

Graphical Identification and Authentication

GPO

Group Policy Object of Active Directory

HA

High Availability

HMAC

Hashed Message Authentication Code

HOTP

HMAC-based One-Time Password algorithm

ICA

Independent Computing Architecture

ICA Client

Another name for **pnagent.exe** (*Start >> All Programs >> Citrix >> MetaFrame Access Clients >> Program Neighborhood Agent*).

IIS

Microsoft Internet Information Server

IMS Bridge

For extending functionalities of third party programs, allowing them to communicate with IMS Server.

IMS Server

An integrated management system that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, authentication policies. provides loss management, certificate management and audit management for the enterprise.

JMX

Java Management Extensions

LDAP

Lightweight Directory Access Protocol

Mobile Active Code (MAC)

A one-time password that is randomly generated, event-based, and delivered via a secure second channel (e.g., SMS on mobile phones).

MOM

Microsoft Operations Manager.

NLB

Microsoft Network Load Balancer

One-Time Password (OTP)

A one-use password generated for an authentication event (e.g., password reset), sometimes communicated between the client and the server via a secure channel (e.g., mobile phones).

Personal Identification Number (PIN)

A password, typically of digits, entered through a telephone keypad or automatic teller machine.

policy

Governs the operation of Encentuate IAM Enterprise, comprising of two (2) main sets: machine policies (managed through Windows GPO) and IMS-managed policies (managed through AccessAdmin).

Radio Frequency Identification (RFID)

A wireless technology that transmits product serial numbers from tags to a scanner, without human intervention.

RADIUS

Remote Authentication Dial-In User Service

RDP

Remote Desktop Protocol

RDP Client

Another name for **mstsc.exe** (*Start* >> *All Programs* >> *Accessories* >> *Communications* >> *Remote Desktop Connection*).

register

Signing up for an Encentuate account, and registering a second factor (e.g., USB Key, RFID) with IMS Server.

single sign-on

A capability that allows a user to enter a user ID and password to access multiple applications.

SOAP

Simple Object Access Protocol

SSL

Secure Sockets Layer

USB Key

A portable and personalized device for storing user names, passwords, certificates, encryption keys, and other security credentials.

user name (user ID)

A unique identifier that differentiates the user from all other users in the system.

Wallet

An identity wallet that stores a user's access credentials and related information (including user IDs, passwords, certificates, encryption keys), each acting as the user's personal meta-directory.